Independent Tests of
Anti-Virus Software

Summary Report 2023

Awards, winners, comments

TEST PERIOD: 2023

LAST REVISION: 15TH JANUARY 2024

WWW.AV-COMPARATIVES.ORG

Contents

Introduction

About AV-Comparatives

We are an independent test lab, providing rigorous testing of security software products. We were founded in 2004 and are based in Innsbruck, Austria.

AV-Comparatives is an **ISO 9001:2015** certified organisation. We received the TÜV Austria certificate for our management system for the scope: "Independent Tests of Anti-Virus Software".

http://www.av-comparatives.org/iso-certification/

AV-Comparatives is the first **certified EICAR Trusted IT-Security Lab** http://www.av-comparatives.org/eicar-trusted-lab/

At the end of every year, AV-Comparatives releases a Summary Report to comment on the various consumer anti-virus products tested over the course of the year, and to highlight the high-scoring products of the different tests that took place over the twelve months. Please bear in mind that this report considers all the Consumer Main-Test Series of 2023, i.e. not just the latest ones. Comments and conclusions are based on the results shown in the various comparative test reports, as well as from observations made during the tests (https://www.av-comparatives.org/consumer/test-methods/).

Tested Vendors

The following vendors' products were included in AV-Comparatives' Public Consumer Main-Test Series of 2023 and had the effectiveness of their products independently evaluated. We are happy that this year's tests helped several vendors to find critical and other bugs in their software, and that this has contributed to improving the products.

Management Summary

Tests

In 2023, AV-Comparatives subjected 16 consumer security products for Windows to rigorous investigation. All the programs were tested for their ability to protect against real-world Internet threats, identify thousands of recent malicious programs, defend against advanced targeted attacks, and provide protection without slowing down the PC.

Results and Awards

Whilst all of the programs in our test reached an acceptable level overall, some programs outperformed others. For details, please see "Overview of levels reached during 2023". In order to recognise those products that achieve outstanding scores in our tests, we have given a number of end-of-year awards that highlight the best results in each test, and overall. The Product of the Year, Outstanding Product and Top Rated Awards are based on overall performance in the Public Consumer Main-Test Series; there are also Gold, Silver and Bronze awards for each individual test type. Please see the Award Winners section for more details of the awards. The 2023 **Product of the Year Award** goes to **Kaspersky. Bitdefender** receives the **Outstanding Product Award**. **Avast**, **AVG, Avira, ESET** and **G Data** win **Top-Rated Awards**.

Overview of tested products

Here we provide a summary for each of the programs tested, with a note of each one's successes during the year. Although the user interface does not affect any awards, we have noted some of the best UI features as well.

Avast takes a **Top-Rated Product Award** in 2023, after reaching Advanced+ level in six out of seven tests, and Advanced for the remaining test. It also receives **Gold Awards** for the **Real-World Protection Test** and **Malware Protection Test**. It has a very clean, modern interface, and the setup wizard offers ideal options for both expert and non-expert users.

AVG receives a **Top-Rated Product Award** for 2023, having reached Advanced+ level in six out of seven tests, and Advanced in the remaining test. It also wins **Gold Awards** for the **Real-World Protection Test** and **Malware Protection Test**. It has a touch-friendly interface and good setup options.

Avira gets a **Top-Rated Product Award** in 2023, after reaching Advanced+ level in six out of seven tests. It also receives **Silver Awards** for the **Malware Protection Test and Performance Test**. The program features a modern, touch-friendly interface, and deleted the source malware files on an external drive in our USB copy check.

Bitdefender is AV-Comparatives' **Outstanding Product** of 2023, having received the highest Advanced+ Award in all seven tests this year. It took the **Gold Award** for the Advanced Threat Protection Test, and also wins a **Silver Award** for the **Real-World Protection Test**, plus a **Bronze Award** for the **Malware Protection Test**. Its well-designed user interface includes a customisable home page, and external drives are automatically scanned on connection.

ESET receives a **Top-Rated Product Award** this year, after receiving five Advanced+ and one Advanced Awards in seven tests. It also takes the **Gold Award** for **Low False Positives**, a **Silver Award** for the **Advanced Threat Protection Test**, and a **Bronze Award** for the **Performance Test**. Reviewers were impressed with the clear and simple layout of the GUI, and ease of use.

F-Secure was successful this year, reaching Advanced level in five out of six tests. It excelled in terms of very rapidly deleting malware samples on USB drives and network shares, thus preventing any chance of them being copied to the system. Testers also noted an easy-to-navigate interface, along with helpful explanations of features.

G Data takes a **Top-Rated Product Award** for 2023, having reached Advanced+ level in four of the year's tests, and Advanced for the other three. It also receives **Bronze Awards** for the **Real-World Protection Test**, **Malware Protection Test**, and **Advanced Threat Protection Test**. Reviewers noted its proactive scanning of external drives, detailed status display, and excellent access control.

K7 gets the **Gold Award** for the **Performance Test** this year, and also took two Advanced+ and two Advanced Awards in the 2023 tests. Its highly sensitive on-access protection detects malware on external drives or network shares as soon as they are opened. Reviewers noted optimal access control, and a simple, easy-to-use interface.

Kaspersky is AV-Comparatives' **Product of the Year** for 2023, having taken the highest Advanced+ award in all seven tests. It additionally receives **Silver Awards** for the **Real-World Protection Test, Malware Protection Test**, and **Advanced Threat Protection Test** along with **Bronze Awards** for **Low False Positives** and the **Performance Test**. In our checks, source malware samples were deleted from USB drives network shares and network shares before they could be copied.

McAfee takes a **Gold Award** for the **Malware Protection Test** this year. It also received five Advanced+ and one Advanced Awards in the 2023 tests. Its user interface is clean, modern and touch friendly, and the McAfee Firewall co-ordinates perfectly with Windows' settings.

Microsoft received two Advanced+ and two Advanced Awards in the year's tests. The product is integrated into Windows 10, and has a simple, unobtrusive interface. Its sensitive on-access protection deletes malware on external drives and network shares when these are opened.

Norton received three Advanced+ and three Advanced Awards in this year's tests. It has a well-designed overall user experience, with detailed malware information accessible from alerts. Access control options are excellent, and its firewall co-ordinates perfectly with Windows' settings.

Panda received two Advanced+ Awards in this year's tests. Reviewers noted its simple interface, and the security-blog feature, which lets you read articles on various IT-security related topics. Although it is a free product, upselling is very subtle and unobtrusive.

TotalAV takes the **Silver Award** for **Low False Positives**, and a **Bronze Award** for the **Malware Protection Test**, this year. It also got three Advanced+ and two Advanced Awards in the 2023 tests. It very rapidly deletes malware samples on USB drives, thus preventing any chance of them being copied to the system. Malware alerts are informative, and let you manage multiple detections from a single dialog box.

Total Defense took two Advanced+ and two Advanced Awards in this year's tests. Its user interface stands out for its simplicity. External drives are automatically scanned on connection, and the program windows lets you see all the other devices you have installed with the same account.

Trend Micro received two Advanced+ Awards in this year's tests. The user interface presents a simple overview, but allows easy access to advanced options. It deleted source malware samples from a USB drive and network share in our checks. Its persistent malware and status alerts stand out, and the online manual is clear and easy to read.

Applicability of results to Windows 11

We used the current released build of Windows 10 for the Consumer Main Series Tests, as well as for the User-Experience Reviews, in 2023. As at December of this year, statistics show that a good two-thirds of Windows users are running Windows 10. We also note that Windows 10 is compatible with the great majority of PC hardware in current use. However, Windows 11 is gaining in popularity, and is now usually provided with new consumer PCs. Windows 11 is fully supported by all the vendors participating in this year's tests. Considering the similarities between Windows 10 and Windows 11 in terms of core system operations and security architecture, the conclusions derived from our assessments for Windows 10 can confidently be extended to Windows 11. The fundamental principles governing the effectiveness of anti-virus software against diverse threats are equally applicable to these two Windows versions, ensuring the relevance of our test results to both operating systems. When Windows 11, or a subsequent version of Windows, gains a position of dominance in the market, we are committed to adapting our testing environment accordingly. This will ensure that our evaluations are always aligned with prevalent operating systems, maintaining the relevance of our assessments to the evolving technological ecosystem.

Advice on Choosing Computer Security Software

There is no such thing as the perfect security program, or the best one for all needs and every user. Being recognized as "Product of the Year" does not mean that a program is the "best" in all cases and for everyone: it only means that its overall performance in our tests throughout the year was consistent and unbeaten. Before selecting a security product, please visit the vendor's website and evaluate their software by downloading a trial version. Our awards are based on test results only and do not consider other important factors (such as available interface languages, price, and support options), which you should evaluate for yourself.

Overview of levels reached during 2023

AV-Comparatives provides a wide range of tests and reviews in comprehensive reports (https://www.av-comparatives.org/consumer/test-methods/). Annual awards for 2023 are based on the Public Consumer Main-Test Series: **Real-World Protection Test**, **Performance Test**, **Malware Protection Test, False-Alarm Test** and the **Advanced Threat Protection Test**.

All the programs tested are from reputable and reliable manufacturers. Please note that even the STANDARD level/award requires a program to reach a good standard, although it indicates areas which need further improvement compared to other products. ADVANCED indicates that a product has areas which may need some improvement, but is already very competent. Below is an overview of awards reached by the various anti-virus products in AV-Comparatives' Consumer Main-Test Series of 2023.

	Malware Protection	Performance	Real-World Protection	ATP	Malware Protection	Performance	Real-World Protection
	March 2023	April 2023	February-May 2023	Autumn 2023	September 2023	October 2023	July-October 2023
Kaspersky	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	***	***
Avast	***	***	***	**	***	***	***
AVG	***	***	***	**	***	***	***
Avira	***	***	***	*	***	***	***
ESET	***	***	**	***	***	***	*
G Data	***	**	***	**	***	**	***
McAfee	***	***	***		***	**	***
Norton	***	***	**		**	***	**
TotalAV	***	***			***	**	**
Microsoft	*	*	***		***	**	**
Total Defense	**	*	***		***	*	**
F-Secure	**	**	**			**	**
K7		***	**			***	**
Panda		***			*	***	*
Trend Micro		**	*			**	*

Key: * = Standard, ** = Advanced, *** = Advanced+

Annual Awards

Awards for individual tests

For each of the test types[1] in the Public Consumer Main-Test Series (Real-World Protection, Malware Protection, Advanced Threat Protection, Performance and False Positives), we give **Gold**, **Silver** and **Bronze** awards, for the first, second and third highest-scoring products, respectively.

Awards for combined scores of all tests

As in previous years, in 2023 we are giving our **Product of the Year Award** to the product with the highest overall scores across all the tests in the Public Consumer Main-Test Series. This depends on the number of Advanced+ awards received in all the tests. As the overall scores are considered, a product can receive the Product of the Year award without necessarily reaching the highest score in any individual test. A product cannot win the Product of the Year Award in two consecutive years if in the second year there is another product (or other products) with the same highest award levels.

We sometimes have a situation where two products reach exactly the same highest award levels. We think it is fair to highlight the fact that more than one product has reached an excellent level, and so in such cases we give the Product of the Year Award to the product that didn't get it most recently. The other product with the same highest award levels will receive the **Outstanding Product Award**. It even happens that three or more products reach the same highest award levels. In this situation, the product with the highest individual scores wins Product of the Year, while the others receive the Outstanding Product Award. In cases of uncertainty, the final allocation of the 'Product of the Year' and 'Outstanding Product' awards will be decided by the tester, considering principally the precise results of the individual tests.

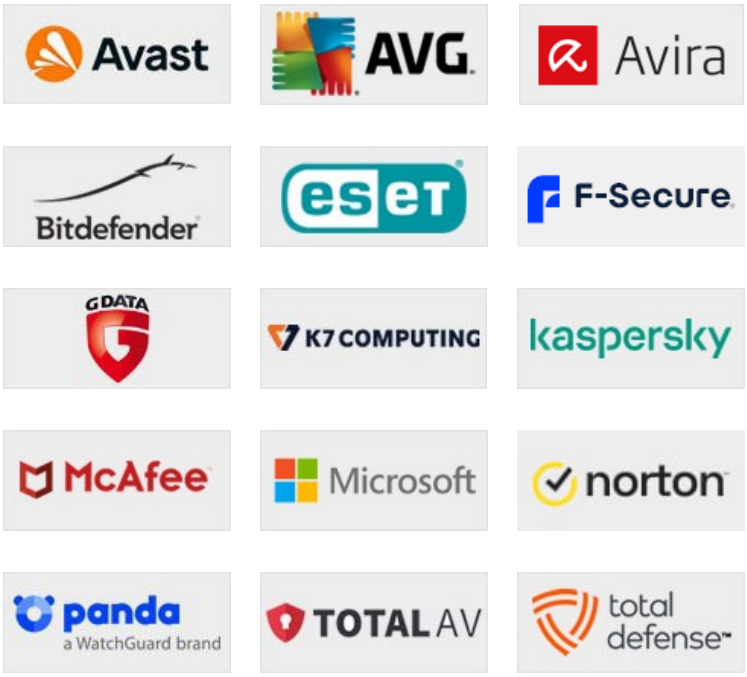
As in previous years, we will also be giving **Top-Rated Product Award** to a select group of tested products which reached a very high standard in the Public Consumer Main-Test Series. We have used the results over the year to designate products as "Top-Rated". Results from all the tests are assigned points as follows: Tested = 0, Standard = 5, Advanced = 10, Advanced+ = 15. Products with 90 points or more are given the **Top-Rated award**.

To get the **Approved Windows Security Product Award**, at least 35 points must be reached.

[1] For some test types, there may be two actual tests conducted in a year; the awards are based on the combined score of both tests.

Approved Security Product Award

The vast majority of products from the 16 vendors tested have earned the prestigious AV-Comparatives 2023 Approved Windows Security Products certification, underscoring their commitment to excellence in security solutions. These are listed below:



Product of the Year 2023

AV-Comparatives' 2023 Product of the Year Award goes to:

Kaspersky

Outstanding Product 2023

AV-Comparatives' 2023 Outstanding Product Award goes to:

Bitdefender

Top-Rated Products 2023

AV-Comparatives' Top-Rated Awards for 2023 goes to:

Avast, AVG, Avira, ESET, G Data

Please see our summary and awards pages – links below:
https://www.av-comparatives.org/test-results/
https://www.av-comparatives.org/awards/

Real-World Protection Test winners

Security products include various different features to protect systems against malware. Such protection features are taken into account in the Real-World Protection Test, which tests products under realistic Internet usage conditions. Products must provide a high level of protection without producing too many false alarms, and without requiring the user to make a decision as to whether something is harmful or not.

The programs with the best overall results over the course of the year were from: **Avast, AVG, Bitdefender, Kaspersky** and **G Data**.

AWARDS

Avast, AVG

Bitdefender, Kaspersky

G Data

For details and full results of the 2023 Real-World Protection tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/real-world-protection-tests/

Malware Protection winners

The Malware Protection Test evaluates an AV product's ability to protect against malware coming from removable devices or network shares. Products must provide a high level of protection without producing too many false alarms. In the Malware Protection Test, all samples not detected on-demand or on-access are executed.

Avast, AVG, McAfee, Avira, Kaspersky, Bitdefender, G Data and **TotalAV** scored well in both tests.

AWARDS

Avast, AVG, McAfee

Avira, Kaspersky

Bitdefender, G Data, TotalAV

For details and full results of the 2023 Malware Protection tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/malware-protection-tests/

False Positives winners

False positives can cause as much trouble as a real infection. Due to this, it is important that anti-virus products undergo stringent quality assurance testing before release to the public, in order to avoid false positives. AV-Comparatives carry out extensive false-alarm testing as part of the Malware Protection Tests. Additionally, also false alarms from the Real-World Protection Test are counted for this category.

The products with the lowest rates of false positives during 2023 were **ESET** (2), **TotalAV** (9) and **Kaspersky** (10). These figures represent the SUM of the false positives from all False Alarm Tests.

AWARDS

ESET

TotalAV

Kaspersky

False Alarm Testing is included in each Protection Test.

For additional details about False Positives in the Malware Protection Test, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/false-alarm-tests/

Overall Performance (Low System-Impact) winners

Security products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks.

K7, AVIRA, ESET and **Kaspersky** demonstrated a lower impact on system performance than other products.

AWARDS

K7

Avira

ESET, Kaspersky

For details and full results of the 2023 Performance Tests, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/performance-tests/

Advanced Threat Protection (Enhanced Real-World Test) winners

This tests a program's ability to protect against advanced targeted and fileless attacks.

Bitdefender blocked 14 targeted attacks (out of 15), while **ESET** and **Kaspersky** blocked 13 attacks, and **G Data** blocked 12 attacks.

AWARDS

Bitdefender

ESET, Kaspersky

G Data

For details and full results of the 2023 Advanced Threat Protection Test, please click the link below:
https://www.av-comparatives.org/consumer/testmethod/advanced-threat-protection-tests/

Pricing

AV-Comparatives' awards and rankings are based entirely on products' technical capabilities, not on any other factors such as costs. However, the price of a security product is obviously a factor that users consider. We have listed here some considerations that readers may like to take into account when choosing their security software.

We would not recommend choosing a security product based on price alone. We suggest that you look at protection, performance and ease of use first, and consider the price last.

It is clear that some free programs' protection and performance are on a par with paid-for programs, and are easy to use. One of the main disadvantages to free programs can be limited technical support, however. Additional features may also be lacking or limited. Finally, some free programs make extensive advertising for their paid-for counterparts, which many users may find irritating.

It is possible to buy security programs from third-party vendors (e.g. online or in electronics stores) more cheaply than the vendor's list price. We would advise users to check that they are buying the latest version of the product, or that the product purchased can be upgraded to the latest version without additional cost.

When purchasing a product from the vendor's own website, there are two factors that users might like to consider. The first concerns multi-platform licences. Many vendors now offer a licence for e.g. 5 devices, which you can use for Windows, macOS or Android devices, or a mix. In some cases, the price may vary depending on which section of the website you buy from. For example, a multi-platform licence bought from the "Products for Mac" page may be a different price from an (effectively identical) product bought from the "Products for Windows" page.

The second point to consider is auto-renewal. Some vendors offer or automatically apply auto-renewal of the subscription when you buy from their website. Unless you cancel this, you will be charged again at the end of the initial licence period, and the subscription will be extended accordingly. Clearly this is to the advantage of the vendor, as it makes it easy for them to keep you as a customer. If you buy an AV product from the vendor's own website, we suggest that you check the auto-renewal situation first. Some vendors do not have auto-renewal at all. Others let you opt in by putting a tick in a checkbox, while others have auto-renewal activated by default, but let you opt out easily by removing the tick from the checkbox. In some cases, auto-renewal is automatically applied, and cannot be deactivated at the time of purchase; you have to message the vendor afterwards to cancel it. This gives the vendor the opportunity to try to keep you as a customer, by offering various incentives. Most vendors offer the first year at about half the price of what they charge for subsequent years with auto-renewal.

Before agreeing to purchase a product with auto-renewal, we suggest that you find out what the renewal price will be when your subscription expires. In some cases, this may be very much higher than the initial purchase price. However, it might also be cheaper. It is also possible that if you opt out of auto-renewal at the time of purchase, the price shown in the basket will increase. Although also our Security Survey[2] indicates that most users are not happy with mandatory auto-renewal, more and more vendors are nowadays imposing mandatory auto-renewals.

[2] https://www.av-comparatives.org/surveys/it-security-survey-2021/

In the table below we have listed the (rounded) current discount price, full list price and auto-renewal prices (where applicable), including sales tax, for the paid products in the 2023 Main-Test Series.

Product	Devices	Discounted[3] price first year (in EUR incl. VAT)	Full List Price (in EUR incl. VAT)	Auto-renewal price (in EUR incl. VAT)	Auto-renewal ON by Default
Avira Prime	**5**	60 €	105 €	105 €	Yes (mandatory)
Bitdefender Internet Security	1	35 €	50 €	50 €	Yes (mandatory)
ESET Internet Security	1	n/a	40 €	40 €	Yes (optional)
G Data Total Security	1	n/a	50 €	50 €	Yes (optional)
K7 Total Security	1	16 €	26 €	n/a	No
Kaspersky Standard	1	18 €	35 €	35 €	Yes (mandatory)
McAfee Total Protection	1	65 €	150 €	150 €	Yes (mandatory)
Norton AntiVirus Plus	1	15 €	35 €	35 €	Yes (mandatory)
TotalAV Antivirus Pro	**3**	29 €	119 €	119 €[4]	Yes (mandatory)
Total Defense Essential Antivirus	**3**	34 €	57 €	57 €	Yes (mandatory)
Trend Micro Internet Security	1	20 €	50 €	50 €	Yes (optional)
VIPRE Advanced Security	1	35 €	46 €	46 €	Yes (mandatory)

Key: Ratio of rounded autorenewal price to rounded discounted first-year price is (green) no more than twice; (yellow) more than twice but no more than three times; (red) more than three times.

Where "Auto-renewal on by default" is shown as "optional", it means that auto-renewal is activated by default, but can be deactivated at the time of purchase, e.g. by removing a tick/checkmark in the relevant box. Where it is shown as "mandatory", you cannot deactivate it at the time of purchase, but have to cancel it afterwards. Each vendor has its own procedure for deactivating auto-renewal, so we suggest that readers find out about this in good time before the renewal date. It might be that e.g. uninstalling the product from the computer makes cancelling auto-renew more difficult.

The aim of this table is to get an overview about each product's full list price with both its discounted price for the first year and its renewal price for the second year of the subscription. We advise readers NOT to use the data here to compare prices between products. Some products provide just malware protection, whilst others include e.g. parental controls as well, so it would not be a fair comparison. Our 2023 Consumer Main-Test Series tested free products by Avast, AVG, Microsoft and Panda. These products are not shown in the table, as pricing does not apply to them. For three of the products shown in the table, the lowest-price subscription allows you to install the product on more than one device. If you only want to protect one device with these products, you will still have to pay the price shown here. We have given the prices shown on the respective vendor's website at the time of writing (December 2023), applicable to users in Austria. In 2021, the UK's consumer watchdog published guidelines for AV vendors on acceptable practice for auto-renewal. For further details, please see our blogpost[5]. In 2022, similar guidelines were released in Germany[5].

Although the majority of vendors make auto-renewal mandatory, we should point that most commendably, ESET, G Data, K7 and Trend Micro do not impose auto-renewal on users.

[3] It is possible that some vendors may offer additional discounts at specific times or under specific circumstances.

[4] Please be aware that TotalAV stands out by implementing an uncommon pricing strategy, imposing a heightened fee of 165€ annually starting from the third year.

[5] https://www.av-comparatives.org/av-comparatives-welcome-uk-guidelines-on-auto-renewal-by-antivirus-vendors/ and https://www.ecommerce-verbindungsstelle.de/einkaufen-im-internet/online-vertraege-und-abos-kuendigen.html

Trial version availability

The landscape of accessing antivirus trial versions has significantly transformed, departing from its former simplicity of anonymous usage for a set duration. Previously, users could freely download trial versions without the need to disclose payment details or personal information. However, today[6], accessing these trials frequently involves sharing sensitive payment information, such as credit card data, potentially leading to automatic charges once the trial concludes. Furthermore, vendors commonly request personal details like email addresses and phone numbers, which might expose users to subsequent promotional emails or unwanted solicitations aimed at pushing product purchases. This evolution in trial procedures not only complicates the initial user experience but also raises concerns about privacy and unwarranted marketing intrusions.

Product	Requires Payment Information	Requires Account Registration
Avast Free Antivirus	**No**	No
AVG AntiVirus Free	**No**	No
Avira Prime	**YES**	Yes
Bitdefender Internet Security	**No**	Yes
ESET Internet Security	**No**	Yes
F-Secure Internet Security	**No**	Yes
G Data Total Security	**No**	Yes
K7 Total Security	**No**	Yes
Kaspersky Standard	**YES**	Yes
McAfee Total Protection	**YES**	Yes
Microsoft Defender Antivirus	**No**	No
Norton Antivirus Plus	**YES**	Yes
Panda Free Antivirus	**No**	No
TotalAV Antivirus Pro	**YES**	Yes
Total Defense Essential Antivirus	**No**	Yes
Trend Micro Internet Security	**No**	No

Requires Payment Information: This may include details such as credit/debit card information or PayPal account. Users may face automatic charges after the trial period if the otherwise-applicable subscription is not cancelled.

Requires Account Registration: This may involve providing or creating an account with personal details like name, email, password, mobile phone number, and country. Users might receive promotional emails or calls to encourage product adoption. For trial purposes, users could try to use pseudonyms and disposable/fake email addresses to maintain privacy.

Whether users have to provide payment or account information might vary from country to country (e.g. McAfee).

The four free products in the table above do not require personal information in order to get the product. It is commendable that Trend Micro does not require any information to use the trial.

In some cases (e.g. ESET, Trend Micro), the trial cannot easily be found on the localized main product pages.

In the case of TotalAV, there is no real trial offered; users must buy the product but can cancel within 30 days. It is important to mention that all vendors in the list above offer a 30- or 60-day money-back guarantee.

[6] As of December 1st, 2023. We searched for trials on the main product pages of the international/global and various localized websites.

Help and support for technical issues

One reason for purchasing an AV product, as opposed to using a free one, is that help and extended support options for technical issues are included in the licence fee. Effective support from the vendor can be hugely valuable in solving any sort of technical issue with the product. Whilst you might not need it that often, when you do need it, it's really good to have it. If you are using a product, and the vendor does not provide effective support when you need it, you might want to consider using a different product instead.

For clarity, we would define the difference between "help" and "support" as follows. By "help" we mean manuals, online help pages, FAQs and chat bots, where you can access previously-prepared answers and instructions. By "support" we mean communication with a member of the vendor's staff (via email, chat, phone), where you can ask for assistance with your specific problem. User forums may or may not fall into the category of vendor support. In some cases, you may get a reply from an official representative of the vendor, whereas with others you can only ask other users.

Before buying a security solution, you might like to investigate the help and support options provided by the vendor. Here we have noted some things to consider if you do this.

A downloadable user manual is helpful, as it can be used offline. So, if you were having problems accessing the Internet, you could check the manual to see if the product's network protection features might be having any effect on this, and reconfigure them if necessary.

Some vendors offer a free malware-removal service with their products. This is likely to be cheaper than going to a computer repair shop. Vendors may also offer a "malware-removal guarantee", whereby if your computer is infected and the vendor cannot remove the malware, you get back the money you paid for the product.

We note that some help and support options require you to log in to the vendor's online account before you can use them. In such cases, you might not be able to see what options are available until you actually purchase the product. Some vendors make it quite difficult to find contact options for e.g. phone support; you may have to click your way through a number of other pages to find them. You might also find that a vendor additionally offers a premium support service, but if you have purchased the product, you should be entitled to support as part of the licence fee.

Many vendors have different websites for different countries. In some cases, you may have to contact the support service in the country whose website you purchased the product from. Help and support options available for a product may vary from country to country. You should also consider that for telephone support, you may have to call a number in another country, which could mean higher telephone charges. Also, you might not get support in your native language, and you might have to call at an inconvenient time for you, if the vendor only provides support e.g. during their own office hours.

Sorry, AV-Comparatives does not provide technical support for any product. However, if you need assistance with your AV product, we have listed below some of the English-language help and support options for the products in our Consumer Main-Test Series. You can click on the links to go directly to the relevant pages of the respective products' websites.

Product	Online Help	Support Forum	Contact Support
Avast Free Antivirus	Online Help	Avast Forum	n/a
AVG AntiVirus Free	Online Help	AVG Forum	n/a
Avira Prime	Online Help	Avira Forum	Contact
Bitdefender Internet Security	Online Help	Bitdefender Forum	Contact
ESET Internet Security	Online Help	ESET Forum	Contact
F-Secure Internet Security	Online Help	F-Secure Forum	Contact
G Data Total Security	Online Help	n/a	Contact
K7 Total Security	Online Help	K7 Forum	Contact
Kaspersky Standard	Online Help	Kaspersky Forum	Contact
McAfee Total Protection	Online Help	McAfee Forum	Contact
Microsoft Defender Antivirus	Online Help	Microsoft Forum	n/a
Norton Antivirus Plus	Online Help	Norton Forum	Contact
Panda Free Antivirus	Online Help	Panda Forum	n/a
TotalAV Antivirus Pro	Online Help	n/a	Contact
Total Defense Essential Antivirus	Online Help	n/a	Contact
Trend Micro Internet Security	Online Help	Trend Micro Forum	Contact

User-Experience Reviews

Review Format

The aim of the user-experience review is to give readers an idea of what each tested product is like to use in everyday situations. For each of the tested products, we have looked at the following points (where applicable).

About the program

To start off with, we state whether the program is free or has to be paid for. We don't list individual protection components (e.g. signatures, heuristics, behavioural protection), for the following reasons. Our protection tests verify how well each program protects the system, whereby it is not important which component(s) are involved. It is not the number of features that is important, but how effectively they work. Also, different vendors may have different names for individual functions, or combine multiple types of functionality under one name. This could make it misleading to compare products using the vendors' component names. For readers' convenience, we do note any non-malware-related features, such as parental controls or spam filtering. With the exception of a replacement firewall (see below), we do not check the functionality of these additional features.

Setup

We note any options available, whether you have to make any decisions, and any other points of interest, such as introductory wizards that explain the program's features. We suggest that there should be a simple installation option for non-expert users. If at any stage the user has to make a decision in order to proceed, the options should be explained simply and clearly.

System Tray icon

Here we state what functionality is available from the program's System Tray icon. This can be a convenient way of accessing commonly-used functions, such as scans and updates. A System Tray icon is a standard feature for modern security programs for consumers. We regard it as a very useful means of showing that the program is running. However, we note that by default, Windows 10 hides the System Tray icons of third-party programs, so many non-expert users will probably not see the icon for a non-Microsoft AV app.

Security status alert

Here, we disable the program's real-time protection, and check to see what alerts are shown in the program window or elsewhere. We also look for a quick and easy means of reactivating the protection. An effective status display in the main program window, which shows a clear warning if protection is disabled, is a very standard feature, as is a "Fix-All" button/link with which the user can easily re-enable protection if it is not active. We regard both of these as very important, especially for non-expert users. We suggest that additional pop-up alerts, which the user would see even if the program window were not open, are a desirable bonus.

Malware detection alert

We check what sort of alert each program shows when malware is encountered. To do this, we try to copy some malware samples from a network share to the Windows Desktop of our test PC. If the AV product does not detect the copied malware, we then execute one of the samples (by this stage at the latest, all the tested programs will detect the malware samples used).

At whichever point the malware is detected, we look to see what sort of alert is shown, if the user has to take any action, and how long the alert is shown for. If the message box provides a link to more details, we click on this to see what information is provided. We also note whether multiple alerts are shown when multiple malicious files are detected at the same time.

We regard it as ideal if the malware is deleted or quarantined automatically, without the user having to make a decision on what to do with it. We would definitely recommend that any alert box should NOT include an option to instantly whitelist the file (i.e. allow it to be executed there and then). A much safer option is to quarantine the file, after which power users could go into the program's settings to whitelist and restore it if they wanted.

We suggest that persistent alerts, which are displayed until the user closes them, are ideal, as they ensure the user has time to read them. If a separate alert box is shown for every malicious file discovered, it can be a nuisance to have to close them all when multiple detections are made at once. We would say that a single alert box that lets you browse through detections, but can be closed with a single click, is optimal.

Malware detection scenarios

As part of our review, we check to see how each AV program handles malicious programs – at which stage they are detected, what action is taken, and what alerts are shown – in four different scenarios. These are: execution; copying from a USB drive to the system; copying from a shared network folder to the system; on-demand scan of a USB drive via Windows Explorer's right-click menu. For all of these, we use the same set of files, made up as follows. We take 5 highly prevalent malware samples, and 5 clean files (current installers for popular Windows programs). We then copy all 10 files into a sub-folder, to see if these are handled differently by the AV program from those in the root directory. The entire set of 20 files is then copied to a USB flash drive or network share, as applicable.

The USB copy and LAN copy checks allow us to see if the AV product has on-access protection (meaning the copied malware will be detected during or shortly after the copy process), or on-execution protection (meaning that malicious files can be copied to the system, but will be detected as soon as they are run). Regarding on-access versus on-execution protection, we suggest that for most people, the former is the better option. Whilst it may have a somewhat higher effect on system performance, it helps ensure that users cannot inadvertently pass on malware to other people, e.g. by copying it to a flash drive or network share, or sending it as an email attachment. For the execution check, we disable any automatic USB-scanning function in the AV program, and connect the USB drive (ignoring any prompts to scan it). We then open the drive in Windows File Explorer, and attempt to run in turn each of the five malware samples on the root of the drive. We have Windows Task Manager running during this check, so that we can observe whether any of the malicious programs is able to start a process. We note that some security programs with very sensitive on-access protection will delete the malware before it can be executed – an ideal action, which renders an actual execution check redundant. In our USB copy check, we attempt to copy the entire set of files from a USB flash drive to the Windows Desktop. Again, we disable/ignore any attempts by the program to scan the USB drive, which we connect to the system and open in File Explorer. To simulate the realistic action/speed of a non-expert user, we allow 10 seconds between opening the drive and starting the copy process, which we perform with Explorer itself. We then note the following: if the malware is deleted from the USB drive, and at which stage if so; if it is possible to copy any of the (remaining) malware to the Desktop; and if the latter is the case, whether the malicious files are later deleted from the Desktop by the AV program.

For the LAN copy check, we follow the same procedure as for USB copy, except that the files are on a writeable network share rather than a flash drive. In many cases, the results – in terms of whether the malicious files can be copied, and how they are then handled if so – are identical to the USB copy check. We therefore only report on this check for programs that either the handle the malware copy differently, or also delete the source malicious files in the shared folder.

In our on-demand scan test, we again disable/ignore any attempts by the program to scan the USB drive, which we connect to the system. Without opening the drive itself, we use the AV program's entry in Windows Explorer's right-click menu to run a scan of the drive. We note how the results are displayed by the security program at the end of the scan, whether any further action is needed by the user, and how easy it is to take this where applicable. We also check to see whether all the malware samples have been deleted from the USB drive.

Scan options

Here we look at the different types of on-demand scan provided by each program, how to access and configure them, set scan exclusions, schedule scans, and what options are provided for PUA detection.

Quarantine

In the program's quarantine function, we look to see what information it provides about the detection location/time and the malware itself, and what options are available for processing it, e.g. delete, restore, etc. .

Access control

For users who do not share their computer with anyone, this section is not relevant. However, if you share a computer, e.g. with your family at home, or colleagues in a small business, you might want to read it. Here we check, if it is possible to prevent other users of the computer from disabling the security program's protection features or uninstall it altogether. There are two ways of doing this. Firstly, access can be limited using Windows User Accounts: users with Administrator Accounts can change settings and thus disable protection, whereas those with Standard User Accounts can't. Alternatively, a program can provide password protection, so that any user – regardless of account type – must enter a password to change settings. Some programs provide both methods, which we regard as ideal. When testing access control, we try to find all possible means of disabling protection, to ensure that any restrictions apply to all of them.

Help

In this section, we take a quick look at whatever help features can be directly accessed from the program itself. Some vendors will have additional online resources, such as manuals and FAQ pages, that can be found by visiting their respective websites.

Logs

Here we note what information is provided in the program's log function.

Firewall

Some of the products in this year's tests have a replacement firewall. That is to say, they include their own firewall, which is used in place of Windows Firewall. For these products, we perform a very simple functionality test, to check that basic functions of their replacement firewalls work as expected. In essence, this just verifies that network discovery, file sharing and incoming Remote Desktop access are allowed on private networks, but blocked on public ones.

For this check, we use a laptop PC with a wireless network adapter, running a clean installation of Windows 10 Professional. It is initially connected to a wireless network that is defined as Private in Windows' network status settings. We share the Documents folder, with read and write permissions for "Everyone", and enable Remote Desktop access. In the Windows settings, we turn on network discovery, file sharing, and incoming Remote Desktop access for Private networks, but turn them all off for Public networks. We then verify that all three forms of network access are working as expected, i.e. allowed for Private networks but blocked for Public ones. We then install the security product with default settings, and reboot the computer. If during installation the third-party firewall in the security product were to prompt us to define the current network as public or private, we would designate it as private at that point. We would also note and report this. After the reboot, we check to see if we can still ping the PC, open and edit a document in its shared folder, and gain Remote Desktop access. We would expect the third-party firewall to allow all these types of access. We then connect the laptop to a new, unknown wireless network, which Windows will automatically define as Public in its own settings. If the third-party firewall were to display its own network-status prompt, we would also choose the public/untrusted option here. Next, we attempt to ping the test laptop (using IPv4) from another computer on the same network, access its file share, and log in with Remote Desktop. We would expect the third-party firewall to block all these forms of access, as Windows Firewall would do.

In our opinion, a third-party replacement firewall in a security program should either adopt Windows' network status and firewall settings automatically, or warn the user that they will need to configure it themselves. This would allow laptop users to e.g. share files when at home, but keep intruders out when using public networks.

We recognise that some users may like to use Windows Firewall – which is a known standard – rather than the third-party firewall in their security product. For such users, it is ideal if the security product's own firewall can be cleanly disabled (i.e. permanently disabled, without security alerts being constantly shown), and Windows Firewall can be activated instead. We check to see if this is possible.

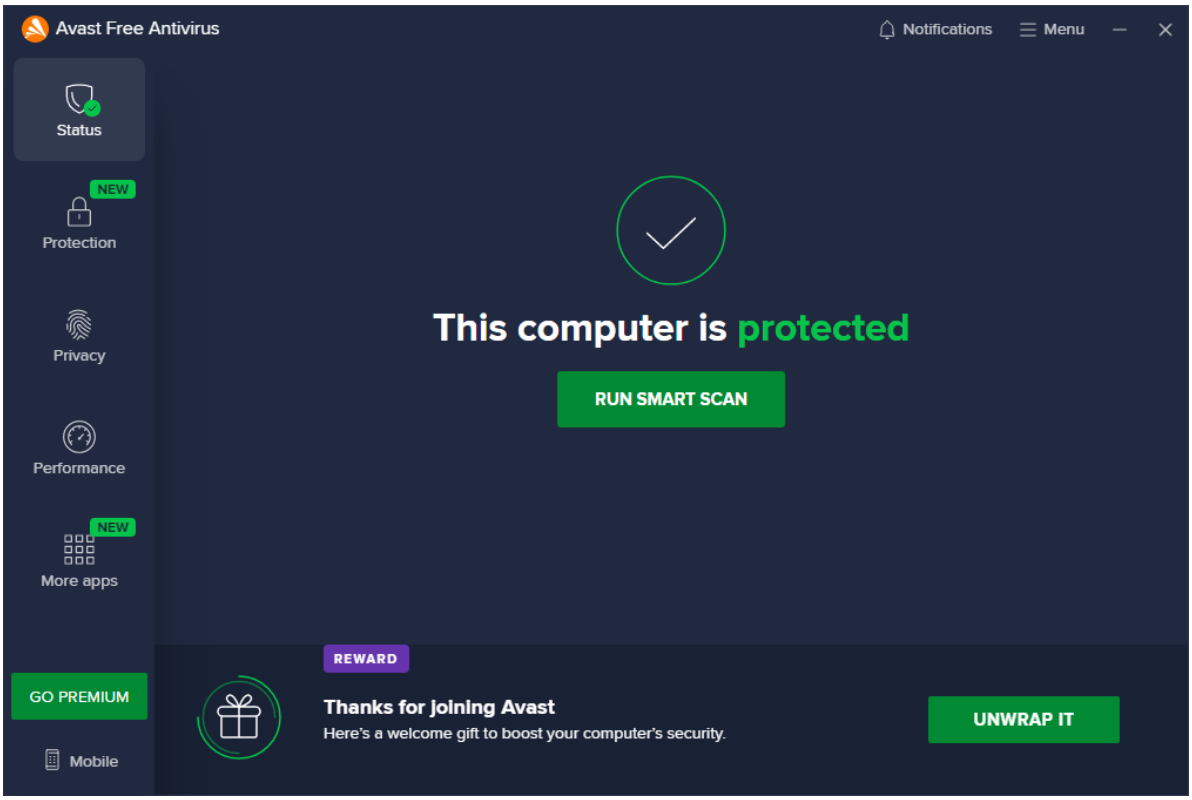
Other points of interest

Here we note anything we observe or find out about a product that we think is relevant. This may include privacy-related items, descriptions of the product on the vendor's website, unusual places to find features, customisation options, prompts to install additional features, upselling, bugs, explanations of functions, and out-of-the-ordinary features and notifications.

Support for Windows 11

All the tests in the 2023 Consumer Main-Test Series were performed using Windows 10. We also used Windows 10 for the review functionality checks described in this section. However, all of the tested/reviewed products are fully compatible/supported with Windows 11.

Avast Free Antivirus



About the program

Avast Free Antivirus is, as its name suggests, a free security program. In addition to anti-malware features, it includes a manual software-updater, a ransomware shield, and a feature that alerts you if the password for a specified online account leaks online. A replacement firewall is available, but is not installed by default. You can find out more about Avast Free Antivirus on the vendor's website: https://www.avast.com/free-antivirus-download

Summary

The interface of Avast Free Antivirus is clean, touch-friendly, and easy to navigate. We liked the informative malware detection alerts, which let you manage multiple detections from a single alert box, and persist until closed by the user. The setup wizard provides the choice of a simple, one-click installation, or a fully customisable installation, making it ideal for both non-experts and power users. There is a good range of scan options, and on-access protection means that files are scanned for malware if you try to copy them to your PC.

Setup

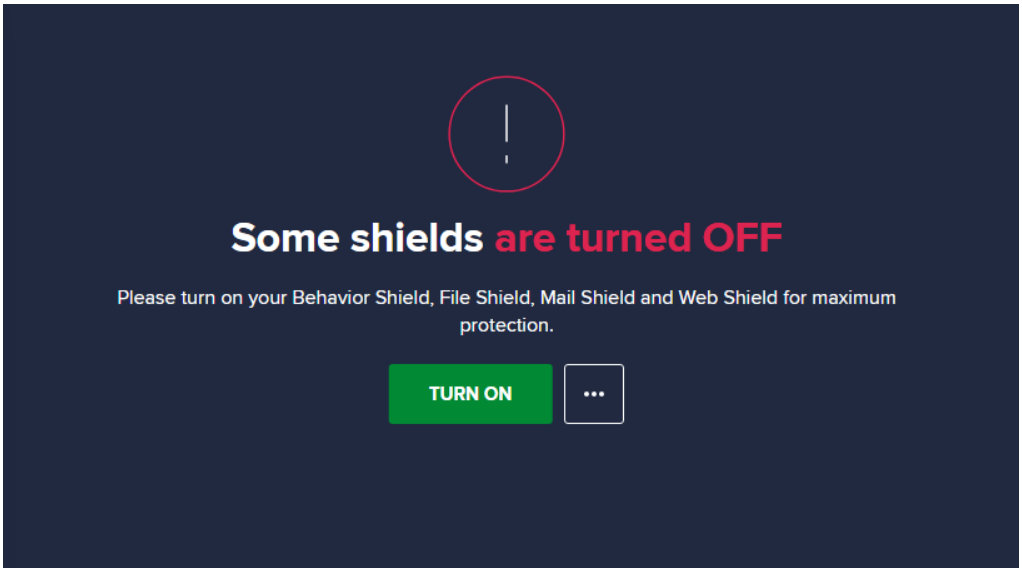
The setup wizard offers to install the *Avast Secure Browser*, and make this the default browser, but you can easily opt out of this by removing the relevant ticks (checkmarks). We chose not to install the Avast browser for our functionality test. The setup wizard also lets you select the interface language, after which you can simply click *Install*. Power users can opt to customize the installation. With this option, you can select individual components to be installed. We used the default configuration. After completing setup, we were shown an option to upgrade to the paid version, and then prompted to run a first scan.

System Tray icon

From the System Tray menu, you can open the program window, disable protection for a specified time, use *Silent Mode*, open quarantine, update the program and/or definitions, and see program and registration information.

Security status alert

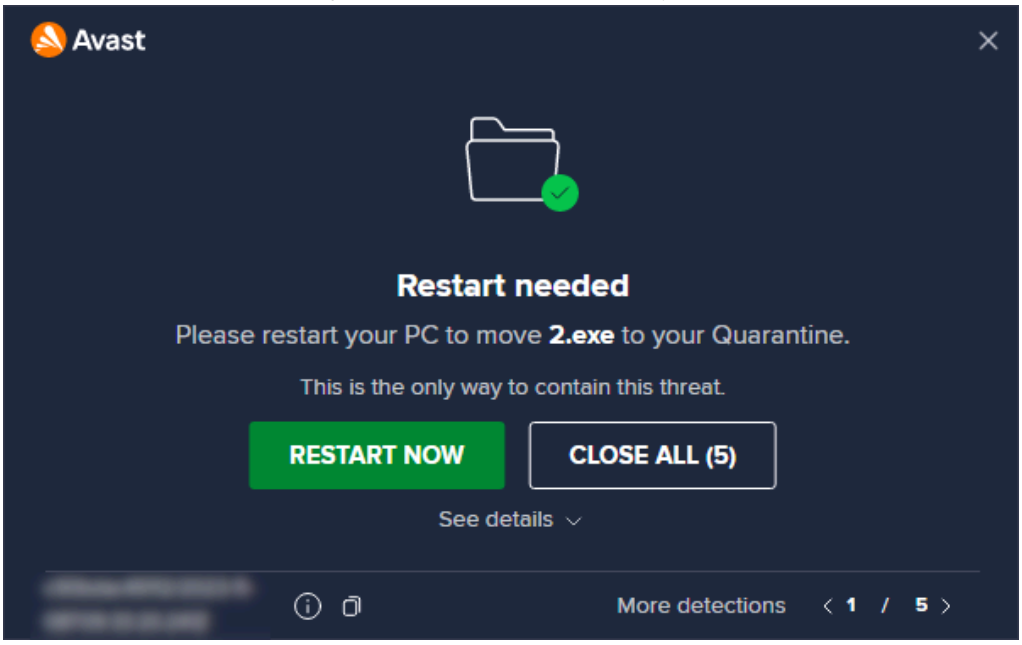
When we disabled real-time protection in the program's settings, an alert was shown on the program's home page (screenshot below). We were able to reactivate the protection easily by clicking *Turn On*.



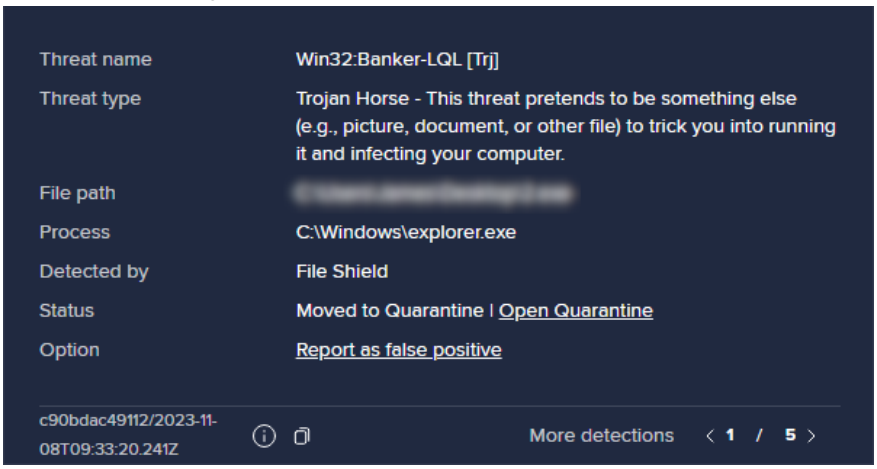
We note that if you click the three dots button, you will get the option *Ignore*. We do not recommend using this, as it permanently deactivates the warning message normally shown when protection is disabled.

Malware detection alert

When a malicious file was detected in our functionality check, Avast displayed the alert shown below. We did not need to take any action. This alert window persisted until we closed it.



Clicking *See details* displayed additional information about the threat, including a brief, simple definition of "Trojan":



Whenever multiple malicious files were detected at the same time, Avast showed a single alert box. There we could browse through the various threats, see details, and close all alerts with a single click.

Malware detection scenarios

We performed an Execution Check with Avast, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process. When we attached a USB flash drive with some malware samples and clean files to our test PC, an Avast pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. Avast did not take any action at this stage. However, when we copied the drive's contents to the Windows Desktop, the malicious files were deleted just a few seconds after the copy procedure had finished. This did not give us enough time to execute any of them, which is obviously good. A single alert box was shown, with the option of seeing details of individual detections. When we scanned the USB drive via Windows Explorer's right-click menu, Avast showed us a list of the malicious files found, including the file names and paths, with the recommendation to quarantine them. We were able to select all the detected threats at once by clicking Select All; there was also the option of selecting individual items via check boxes. We then just had to click Resolve All, and shortly afterwards, Avast informed us that each of the threats had been moved to quarantine. All the malware samples were deleted from the USB drive.

Scan options

The *Smart Scan* button on the home page checks for security vulnerabilities in the OS settings, runs a very quick malware scan, and checks for so-called advanced issues. However, a premium license is required to resolve the advanced issues, and Avast prompts you to purchase a license. The *Protection\Virus Scans* page offers *Full\Targeted\Boot-Time\Custom* scans. A *Custom* scan can be scheduled on a daily, weekly or monthly basis. You can also scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Under *Menu\Settings\Protection\Virus Scans*, you can change the default action to be taken when malware is discovered, and whether to scan for potentially unwanted applications. PUA detection is enabled by default for on-demand scans and real-time protection. Scan exceptions can be configured on the *General* tab of the settings dialog.

Avast's quarantine feature can be accessed from the *Protection* tab. Here you can view a list of all quarantined files along with the threat name and date when it was found. You can select individual files, or all of them, and take one of the following actions: *Delete, Restore, Restore and add exception, Extract, Send for analysis*. The *Extract* function lets you restore the file to a custom location.

Logs

A basic log of scans completed can be found by clicking *Protection/Virus Scans/Scan History*. This shows the date of each scan, along with the detection name, file name/path, and action taken for each detection.

Help

The help feature can be accessed by clicking *Menu\Help\Help*. This opens the support page of the vendor's website, which lists common tasks such as installation, scanning, making exclusions, and uninstallation. For each task, simple step-by-step instructions, along with multiple screenshots, are provided.

Access control

Standard Windows User accounts have full access to the program's settings by default, and so can disable protection features. However, they cannot uninstall the program. If you share your computer, you might like to use the Password feature (under *Menu\Settings\General|Password)*. There are two options for doing this. The *Require password only to access settings* option locks the settings dialog. However, it is still possible to disable protection using the System Tray menu. The second option, *Require password to open Avast and access settings*, makes it impossible to access settings or disable protection by any means. However, it also locks any form of access to the main program window and the functionality of the System Tray menu. The only thing a user can do then is to run a right-click scan from Windows Explorer, though it will not be possible to see the scan results or take any action on malware found.

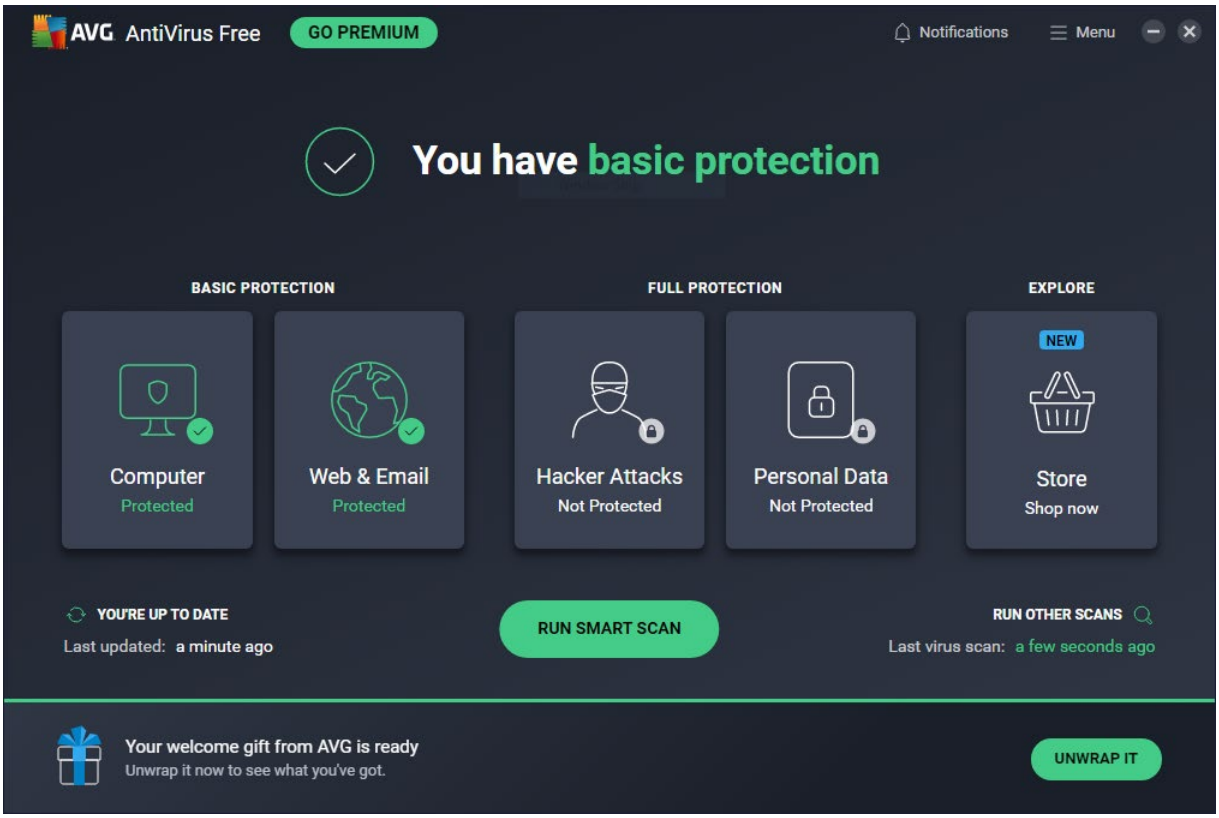
Advertising

The user interface of Avast Free Antivirus actively promotes the paid-for Premium Security product and other security products, in various ways. Some people may find this a considerable irritation. In any event, we would suggest that users obtain independent advice on what other types of security/performance-related programs are appropriate to their needs before buying any additional products.

Other points of interest

- The *Rescue Disk* feature can be found on the *Protection\Virus Scans* page. This allows you to make a bootable CD/DVD/flash drive that you can use to scan and remove malware from an infected PC.
- By default, Avast collects user data via 3rd-party analysis services. However, they inform us that this is only used in-house for e.g. product improvement purposes.

AVG AntiVirus Free



About the program

As the name suggests, AVG AntiVirus Free is a free security program. It offers anti-malware features, as well as a ransomware shield, and a secure delete function. A replacement firewall is available, but is not installed by default. You can find out more about the program on the vendor's website: https://www.avg.com/en-eu/free-antivirus-download

Summary

AVG AntiVirus Free features a modern and touch-friendly interface, which is straightforward to use. We liked the informative malware detection alerts, which let you manage multiple detections from a single alert window, and persist until closed by the user. The setup wizard provides the choice of a simple, one-click installation for non-experts, or a fully customisable install for power users. There is a good range of scan options, and on-access protection means that files are scanned for malware if you try to copy them to your PC.

Setup

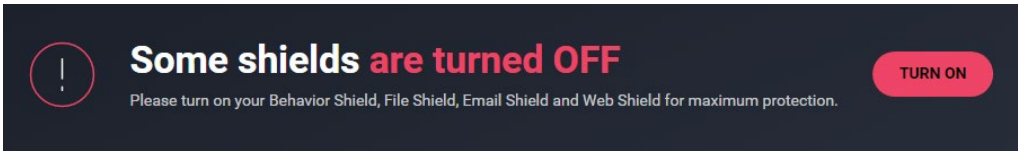
The setup wizard offers to install the *AVG Secure Browser*, and make this the default browser, but you can easily opt out of this by removing the relevant ticks (checkmarks) on the first page of the setup wizard. We chose not to install the AVG browser for our functionality test. The setup wizard also lets you select the interface language, after which you can simply click *Install*. Power users can opt to customize the installation. With this option, you can select individual components to be installed. We used the default configuration. After completing the setup we were shown an option to upgrade to the paid version and then prompted to run a first scan.

System Tray icon

Hovering over the System Tray icon displays the protection status. Right clicking the icon lets you open the program, scan the computer, and disable protection.

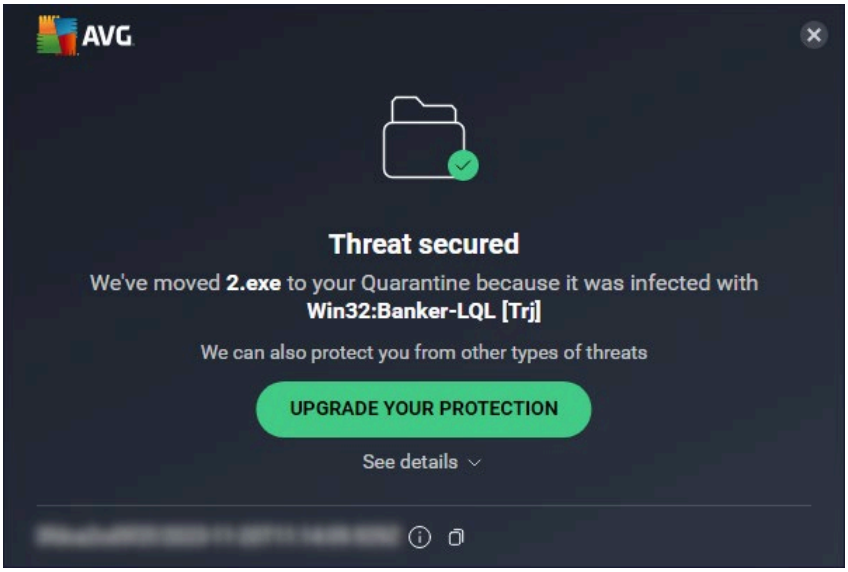
Security status alert

When we disabled protection features, we were prompted to confirm this and to select for how long to disable protection. We appreciated the fact that protection is automatically turned on again. Additionally, an alert was shown on the status page (screenshot below) and *Computer* tile of the main program window. We were able to reactivate the protection easily by clicking *Turn on*.

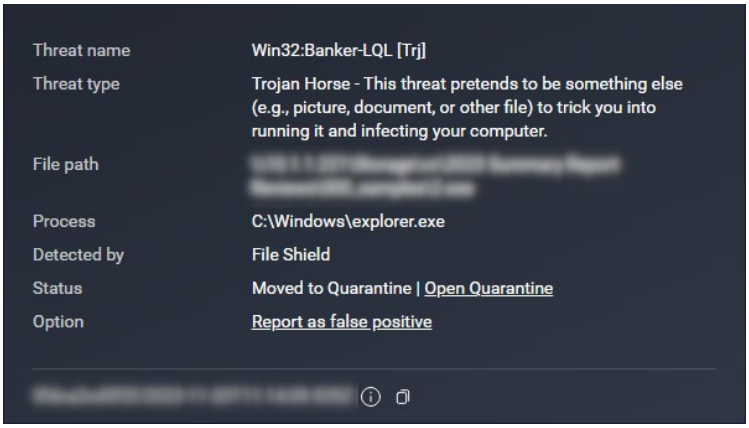


Malware detection alert

When a malicious file was detected in our functionality check, AVG blocked it and displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.



Clicking *See details* displayed additional information about the threat:



Whenever multiple malicious files were detected at the same time, Avast showed a single alert box. There we could browse through the various threats, see details, and close all alerts with a single click.

Malware detection scenarios

We performed an execution check with AVG, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, an AVG pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. AVG did not take any action at this stage. When we then tried to copy the drive's contents to the Windows Desktop, AVG prevented the malicious files from being copied, which we find to be very good. However, no alert was shown.

When we scanned the USB drive via Windows Explorer's right-click menu, AVG showed us a list of the malicious files found, including the file names and paths, and informed us that they had all been quarantined. We feel that this is an optimal solution, as no user decision was required, and file names/locations were shown up front. All the malware samples were deleted from the USB drive.

Scan options

The *Smart Scan* button on the home page checks for security vulnerabilities in the OS settings, runs a very quick malware scan, and checks for so-called advanced issues. However, a premium license is required to resolve the advanced issues and Avast prompts you to purchase a license. The *Protection\Virus Scans* page offers *Full\Targeted\Boot-Time\Custom* scans. A *Custom* scan can be scheduled on a daily, weekly or monthly basis. You can also scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Under *Menu\Settings\Protection\Virus Scans*, you can change the default action to be taken when malware is discovered, and whether to scan for potentially unwanted applications. PUA detection is enabled by default for on-demand scans and real-time protection. Scan exceptions can be configured on the *General* tab of the settings dialog.

Quarantine

AVG's quarantine page can be accessed from Tools section of the *Menu* (you have to scroll down to find it). It shows the file names and detection names of quarantined items, along with their location and date/time of detection. You can select individual files, or all of them, and take one of the following actions: *Delete, Restore, Restore and add exception, Extract, Send for analysis*. The *Extract* function lets you restore the file to a custom location.

Logs

In its default configuration, AVG AntiVirus Free does not create scan logs.

Help

The help feature can be accessed by clicking *Menu\Help*. This opens the product's support page on the vendor's website. Here frequently asked questions, such as installation, uninstallation, scanning, and operating the quarantine function, are answered. For each topic, there are simple, step-by-step instructions, well-illustrated with screenshots.

Access control

By default, Standard Windows User accounts are able to change settings and disable protection features, but not uninstall the program. If you share your computer, you might like to use the *Password* feature (under *Settings\General*). If you choose the *Require password to open AVG and access settings* option, nobody will be able change any settings or disable protection without knowing the password. The program window will be completely inaccessible, and the only action unauthorised users can perform is a right-click scan from Windows Explorer. It will not be possible to see the results, however. The *Require password only to access settings* option locks the settings dialog, but all users can still disable protection from the System Tray menu, or the *Computer* tile on the home page.

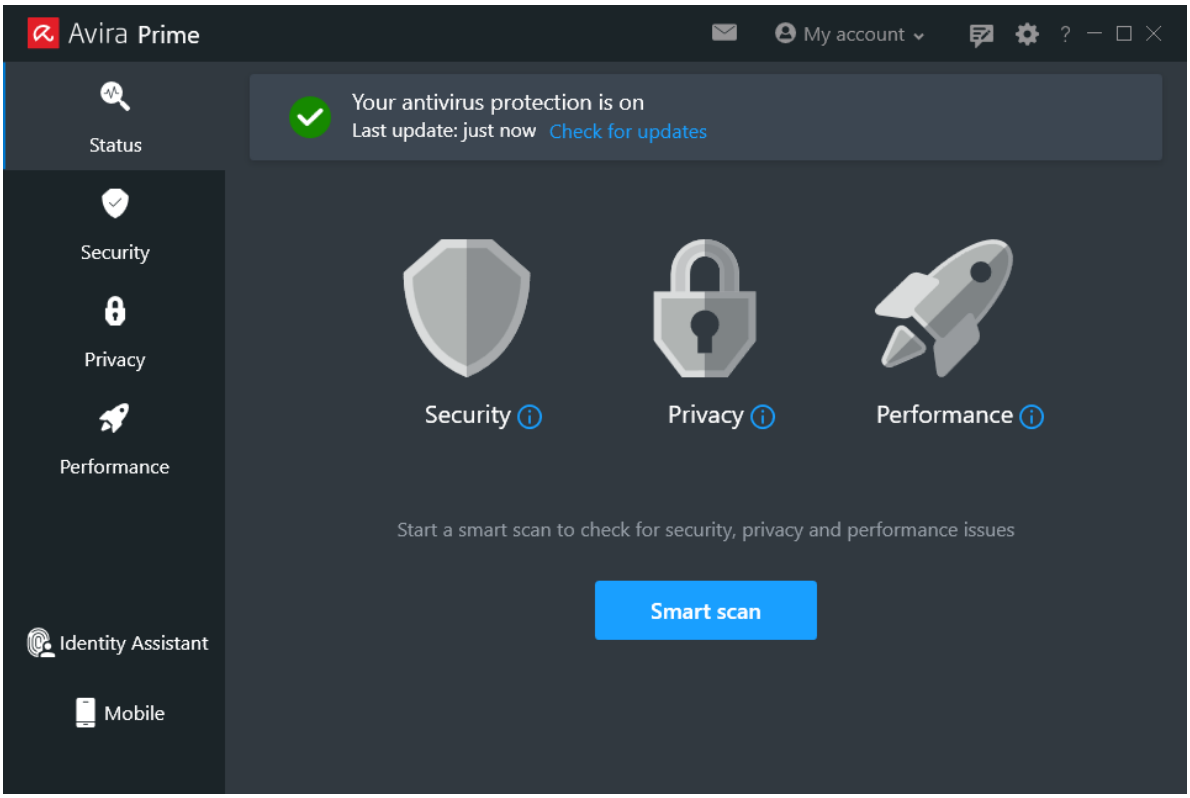
Advertising

The user interface of AVG AntiVirus Free actively promotes other AVG products, including their paid-for Internet Security and Secure VPN. Some people may find this a considerable irritation. In any event, we would suggest that users obtain independent advice on what other types of security/performance-related programs are appropriate to their needs before buying any additional products.

Other points of interest

- The manual update function is found under *Menu/Settings/General/Update*.
- AVG AntiVirus Free includes a hack alert, which monitors your accounts for password leaks.

Avira Prime



About the program

Avira Prime is a paid-for security program. In addition to anti-malware features, it includes a VPN, software updater, privacy settings manager, password manager, file shredder, protection against identity theft, and performance-tuning tools. You can find out more about Avira Prime on the vendor's website: https://www.avira.com/en/prime

Summary

Installing Avira Prime is very straightforward, and the program's simple interface is easy to navigate and offers a choice of light and dark mode. Safe default settings and sensible alerts are provided.

Setup

To set up Avira Prime, log in to your Avira account and download the installer. After launching the installer, only one click is required to complete the setup wizard. Upon finishing, the installer prompts you to run a *Smart Scan*.

System Tray icon

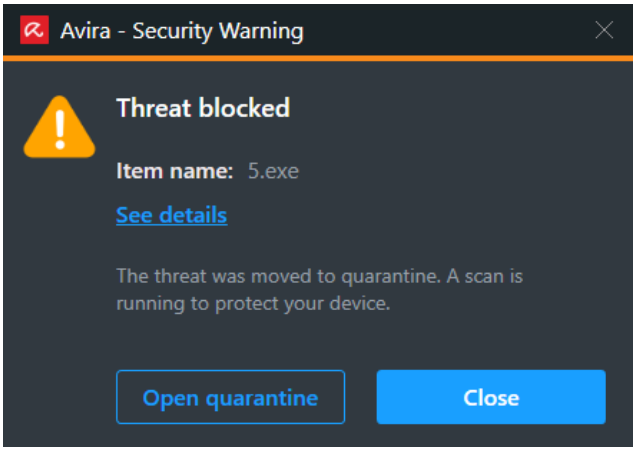
The System Tray icon menu lets you open the program window, run scans and updates, enable/disable real-time protection, activate the VPN, and update the antivirus.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the program's home page. We were able to reactivate the protection easily by clicking *Turn on*.

Malware detection alert

When a malicious file was detected in our functionality check, Avira displayed the message box shown below. We did not need to take any action. The alert persisted until we closed it.



When we clicked on *Open quarantine*, Avira's main program window opened on the *Security\Quarantine* page. When multiple malicious files were detected at the same time, Avira showed just one alert box. Clicking on show details shows more information.

Malware detection scenarios

We performed an Execution Check with Avira, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, an Avira pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. Avira immediately started showing a series of alerts. When we attempted to copy the drive's contents to the Windows Desktop, Avira prevented the malicious files from being copied, and also gradually deleted the source files on the USB drive, which is commendable.

When we scanned the USB drive via Windows Explorer's right-click menu, Avira displayed the notification Threats found: 10. Clicking on See results then showed Threats repaired: 10. A Show details button allowed us to see more information about the malware found in the scan. We consider this to be a good solution, as no user decision was required. All the malware samples were deleted from the USB drive.

Scan options

You can run a *Smart Scan* from the button of the same name on the program's home page. This takes about a minute and checks for privacy and performance issues, viruses, and outdated apps, as well as network threats. Under *Security\Virus Scans* you can choose quick and full scans; both of these can be scheduled. There is also the option to create custom scans. You can additionally scan a local drive, folder or file, by using Windows Explorer's right-click menu. Under *Settings\Security\Virus scans* you can choose which file types and archives to scan, and set scan exclusions. Similar extensive options are also available under *Protection options* for real-time and web protection.

Quarantine

The Quarantine can be reached from the *Security* page. It displays the threat name, file name and path, plus date and time of detection. Quarantined files can be selected individually, or all together, to restore or delete them.

Logs

Under *Security\Virus scans* you can see a record of all scans performed in the past 24 hours. Additionally, the *Quarantine* page shows the date and time of malware detections.

Help

Clicking *Help* in the *?* menu opens Avira's online manuals page. Under *Windows* you will find a searchable FAQ feature. Simple text instructions are offered for the features of Avira Prime, several of which are illustrated with screenshots. There are also explanations of topics such as malware and potentially unwanted applications (PUA).

Access control

Standard Windows User accounts cannot disable protection features, change settings, or uninstall the program. In our opinion, this is as it should be.

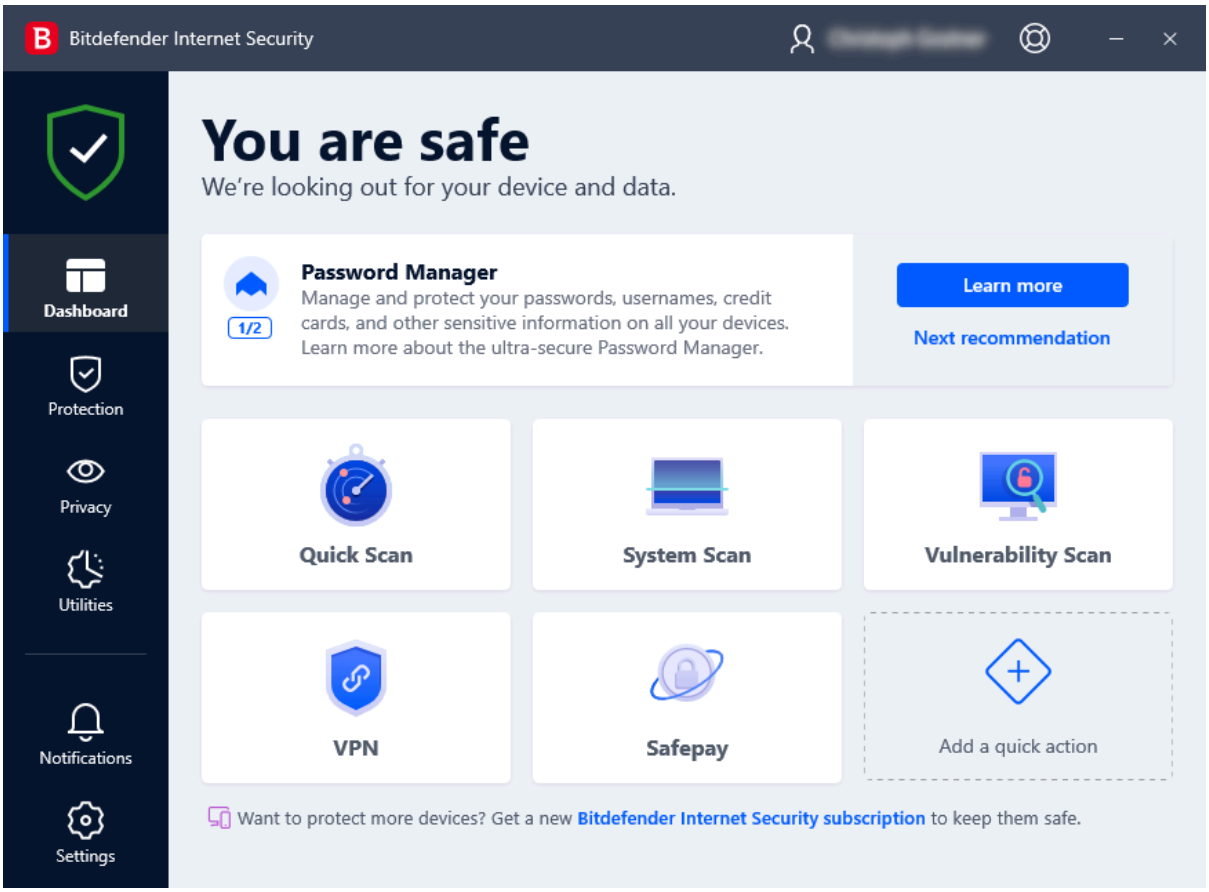
Avira Firewall

In our firewall check, Avira did not reliably protect the test PC in our "public" network. We were able to see its hostname, IPv4 address and MAC address from another computer in the same network (representing a hacker's PC in e.g. a hotel WLAN), using Windows Explorer's Network view. We were also able to make a Remote Desktop connection. We consider this to be a serious security flaw, and that the vendor should rectify it as soon as possible.

Other points of interest:

- Clicking the *?* menu, then *About* shows details about the installed version (including SDK and VDF), license type and expiration date. More subscription information can be found by then clicking on *Manage my licences*. This opens the subscriptions page of your online Avira account.
- At the end of the installation process, Avira prompted us to run a "Smart Scan", which we did. At the end of this scan, the program informed us that there were "7 outdated apps" on our system; we assumed that clicking *Fix issues* would simply update some Windows programs. We then observed that Avira was in fact installing new device drivers and firmware (which had not been offered by Windows Update), rather than applications. Whilst this operation completed successfully, and our test computer continued to function perfectly after the driver/firmware updates, we feel that Avira should be clearer as to what it is actually updating.
- Avira's *Password Manager* add-on is added to Chrome by the setup wizard, although it has to be activated manually.
- Avira Prime offers a light and dark mode, which can be switched in the settings under *General\Language & Appearance*. There is a choice of light and dark modes for the program window, so you can choose whichever you find more readable.

Bitdefender Internet Security



About the program

Bitdefender Internet Security is a paid-for security program. It includes anti-malware features in addition to a replacement firewall, vulnerability scanner, antispam, ransomware remediation, parental controls, file shredder (secure deletion), and a limited VPN. You can find out more about the program on the vendor's website: https://www.bitdefender.com/solutions/internet-security.html

Summary

Bitdefender Internet Security is straightforward to install, easy to navigate, and has good scan options. We liked the option to customise the six tiles on the home page. Most commendably, malware on a USB drive is automatically detected when the drive is connected, and on-access protection means that files are scanned for malware if you try to copy them to your PC. By default, ads for special offers are displayed; in our opinion this should not be the case for a paid product.

Setup

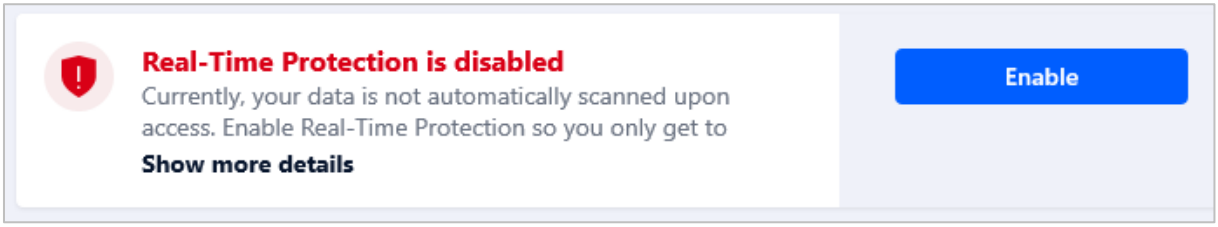
Installation is very straightforward: download the installer from Bitdefender Central and open the file. You then have to accept the Subscription Agreement, but have the option of sending product reports. At the end of setup, an optional "Device Assessment" is suggested. When Bitdefender Internet Security is fist opened a brief tour of the product's main features, which can be skipped, is shown.

System Tray icon

The System Tray icon menu lets you open the program window, see program information, run updates, and show/hide the security widget.

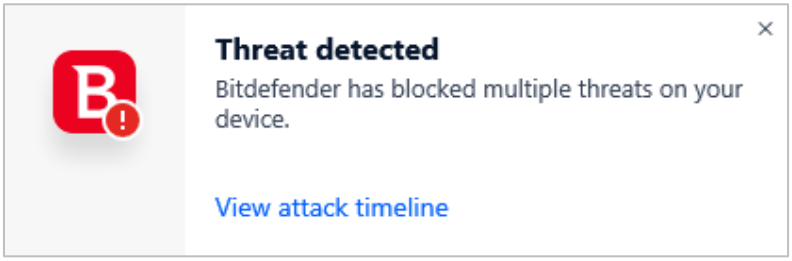
Security status alert

When we disabled real-time protection in the program's settings, the alert in the screenshot below was shown on the home page. We were able to reactivate the protection easily by clicking *Enable Now*.

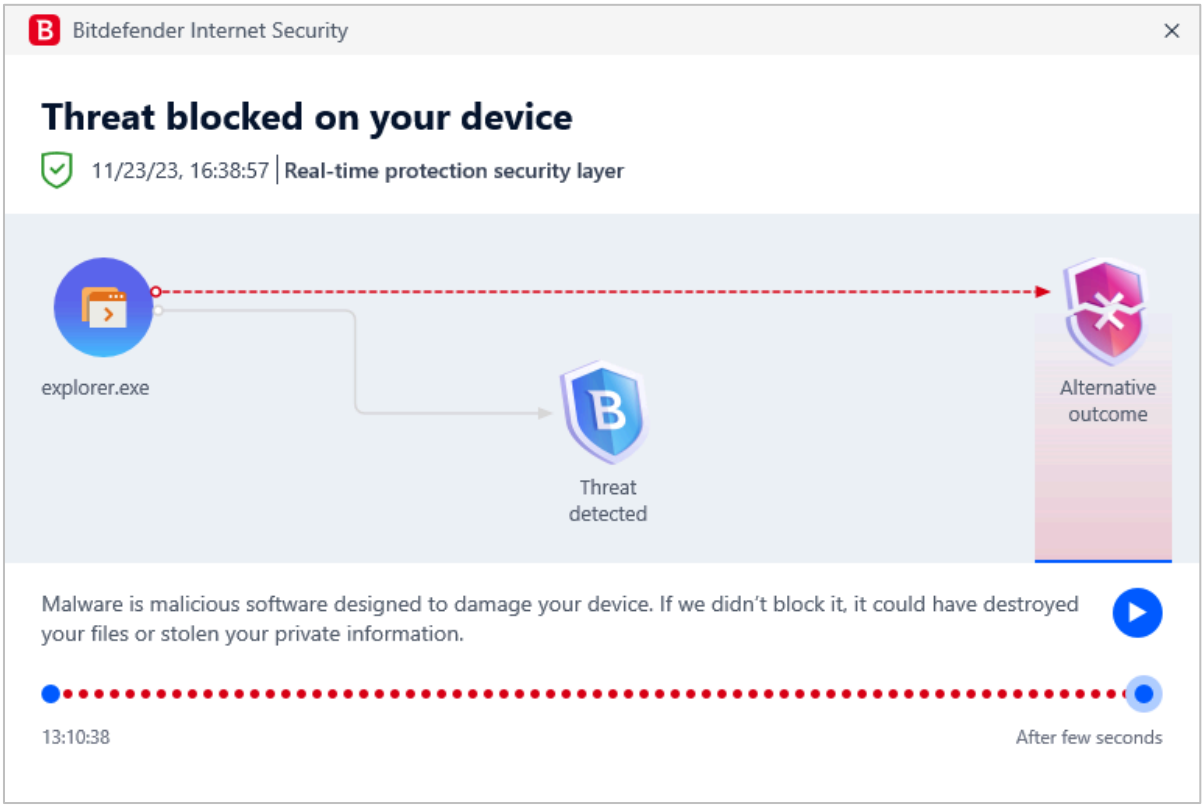


Malware detection alert

After detecting malicious files, Bitdefender displayed the alert shown below. We did not need to take any action, and the alert persisted until we closed it.



When we clicked *View attack timeline* the following window was opened. This shows the Windows processes involved in the detection. For advanced users, this could be a valuable tool for understanding malicious programs and their actions.



When multiple malicious files were detected at the same time, only one alert was shown.

Malware detection scenarios

We performed an execution check with Bitdefender, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, Bitdefender automatically started a scan of the drive – an obviously safe option for non-expert users. This almost immediately detected the malware samples on the drive. In order to conduct our test as planned (i.e. try to copy the drive's contents to the system), we cancelled this scan, disabled automatic USB scanning, and repeated the check with newly copied malware samples. Then, when we opened the drive in Windows Explorer, Bitdefender immediately showed an alert. It prevented the malicious files from being copied to the Windows Desktop, and also gradually deleted the source files on the USB drive, which is commendable.

When we scanned the USB drive via Windows Explorer's right-click menu, Bitdefender showed us a list of the malicious files found, with options to handle all of them the same way, or use different actions for individual files (there was no default option). We selected *Take proper actions* for all files, and clicked *Continue*. Bitdefender then informed us that *Detected threats were resolved*. All the malware samples were deleted from the USB drive.

Scan options

The *Dashboard* page lets you run a *Quick Scan*, *System* Scan, and a *Vulnerability Scan*. Under *Protection\Antivirus\Scans* you can additionally set up a *Custom Scan*. This scan can be scheduled and there is a wide range of options, including whether to scan for potentially unwanted applications, the scan location, whether to scan the memory, if only new and modified files should be scanned, and many more. Scan exceptions can be set on the *Settings* tab of the *Antivirus* page. There you can also open the quarantine, and configure (automatic) scanning of USB drives, optical media, and network drives. You can also scan a local drive, folder or file, or a network share, by using Windows Explorer's right-click menu.

Quarantine

The *Quarantine* page is found under *Protection\Antivirus\Settings* (we feel this is not the most obvious place to put it, and it could be easier to find). It shows the file name and path, detection name, and time/date that each item was quarantined. Items can be selected individually or all at once and then be deleted or restored them.

Logs

Logs can be found on the *Notifications* page, this shows all events that took place. Clicking on individual notifications shows more details. For notification about scans you see full log which details the type of scan and the scan options.

Help

Clicking the lifebelt icon in the top right-hand corner of the window opens the help center. There you can find links to the *User Guide*, *Support Center*, and the *Bitdefender Community*. The *User Guide* is a very comprehensive manual of over 200 pages, covering all aspects of installing, configuring and using the program. There is a glossary of relevant technical terms, and contact details for Bitdefender's support services. The *Support Center* is an online searchable FAQ page. There are detailed instructions illustrated with screenshots and video tutorials.

Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be, in our opinion. You can also password protect the settings, meaning that no other users can disable protection without entering the password.

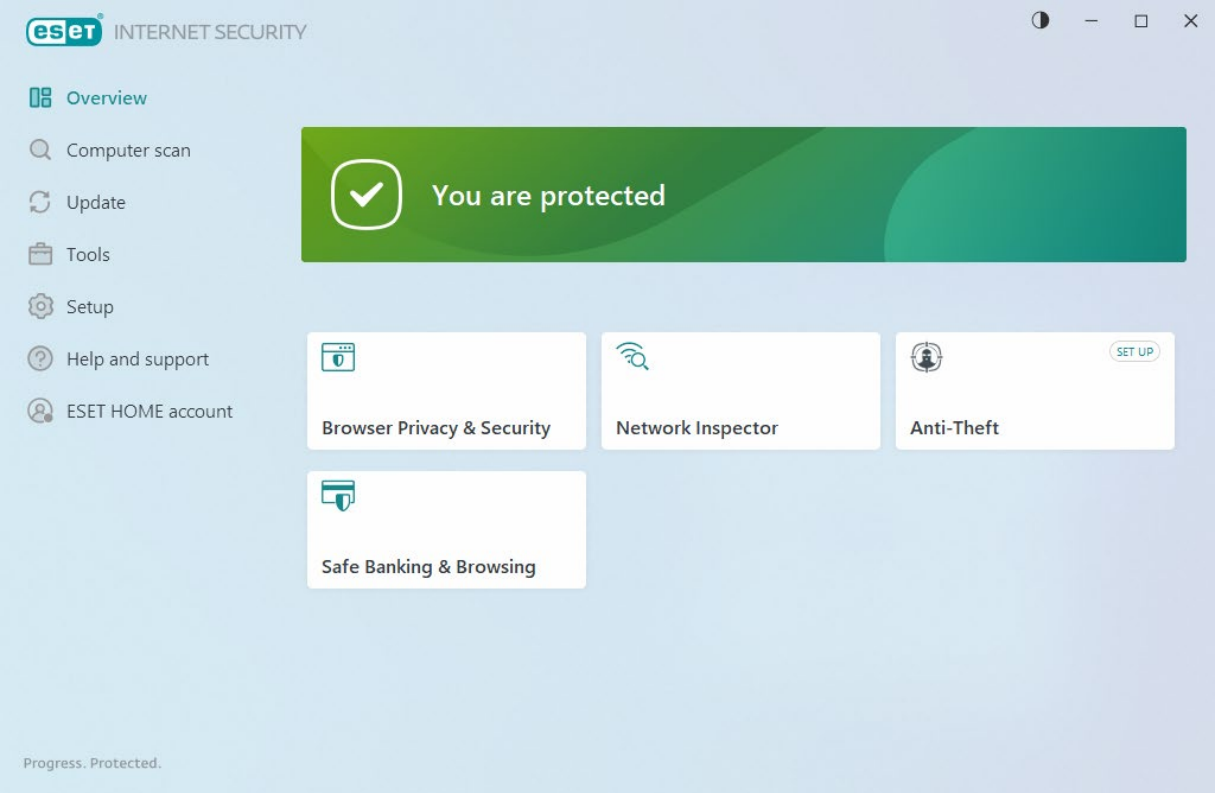
Bitdefender Firewall

During the course of our firewall check, we discovered an issue with the Bitdefender Firewall which could have exposed the device's hostname, IP address and MAC address, and allowed Remote Desktop and file-share access, in a public network. We informed Bitdefender, who immediately investigated and released an updated version of the product to resolve the problem. We rechecked the updated program release, and found that it functioned exactly as it should. It hid the device in public networks, and prevented file-share/Remote Desktop access, but allowed such access in private networks.

Other points of interest:

- Subscription information can be found on the *My Account* page (user menu).
- You can customise which tiles are shown on the *Dashboard* (home page).
- Setup installs the *Bitdefender Anti-Tracker* extension for Chrome.
- By default, the *Special Offers* option is activated. During our testing, a large notification for a sale was displayed. This notification persisted until we closed it.

ESET Internet Security



About the program

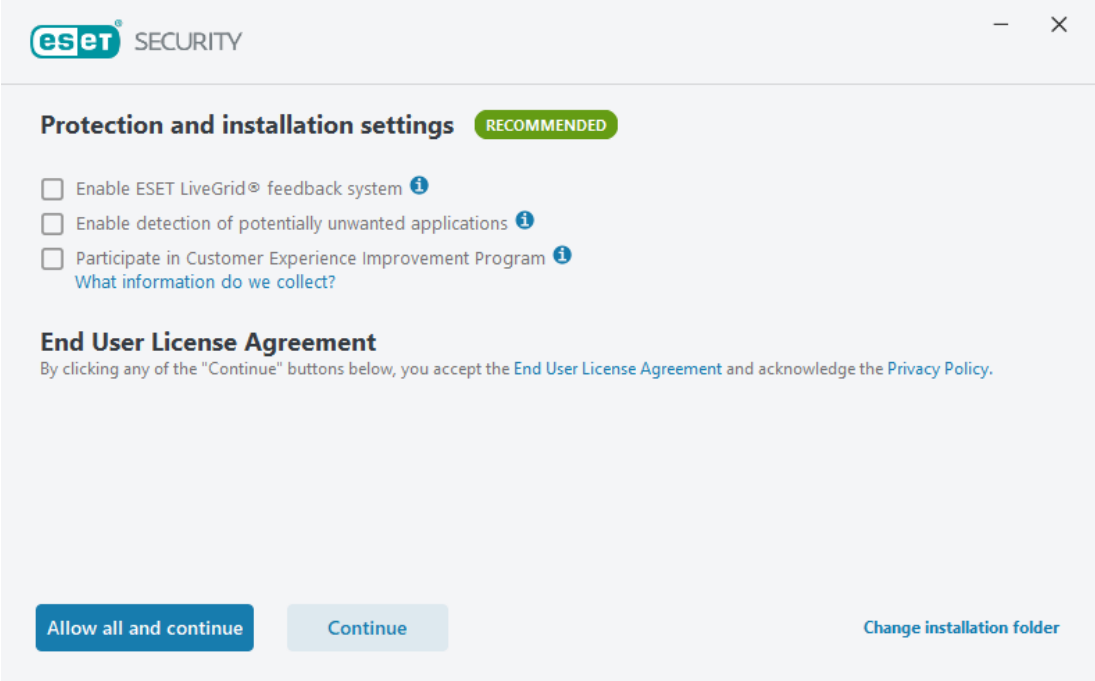
ESET Internet Security is a paid-for security program. In addition to anti-malware features, it includes the ESET Firewall, Network Inspector, Anti-Theft, Anti-Spam, Anti-Phishing, and Banking & Payment Protection. ESET Internet Security is now part of the ESET HOME Security Essential subscription plan. You can find out more about the program on the vendor's website: https://www.eset.com/int/home/internet-security/

Summary

We found ESET Internet Security to be very well designed and easy to use. Non-expert users are provided with safe default settings and a clean, easy-to-navigate interface. All the essential features are very easily accessed. The settings dialog has plenty of advanced options for power users, and offers a useful search function. Help features and access-control options are both excellent. In our functionality check, sensitive on-access protection detected malware on an external drive as soon as it was opened in File Explorer.

Setup

The first page of the installation wizard lets you choose the interface language and provides helpful links to installation instructions and the user guide. In the next step you can enable *LiveGrid* (data sharing), PUA detection, and the *Customer Experience Improvement Program*. In our opinion the button layout is misleading at this point, the dark blue *Allow all and continue* button suggests that this button must be pressed. However, clicking *Continue* also accepts the license agreement and installs the program.



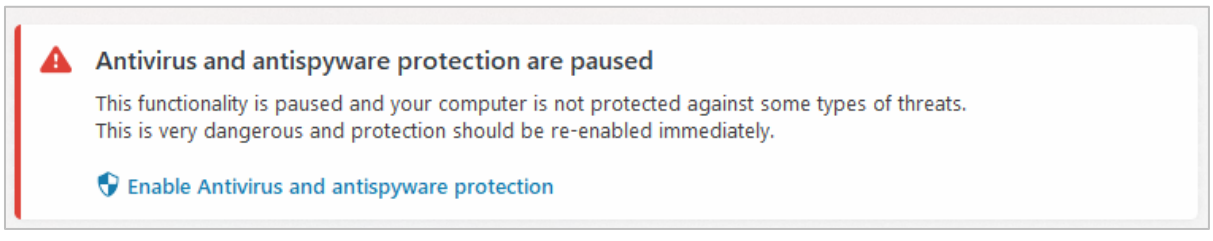
Next, you can login to your ESET HOME account or press *Skip login* to activate the product using a purchased licence key, or to start the free trial period. After activation, the product is installed. On first launch, ESET Internet Security provides you with a brief tour of the product, and an initial scan of the computer is started. Depending on the device's specs, this may take some time, but it can be stopped. The program also invites you to connect the computer to an ESET HOME online management account, although this is optional. The browser plugin *ESET Browser Privacy & Security* is automatically installed as well.

System Tray icon

The System Tray icon menu lets you see protection status, pause protection and firewall, block all network traffic, open settings, see log files, open the program window, see program information, and check for updates.

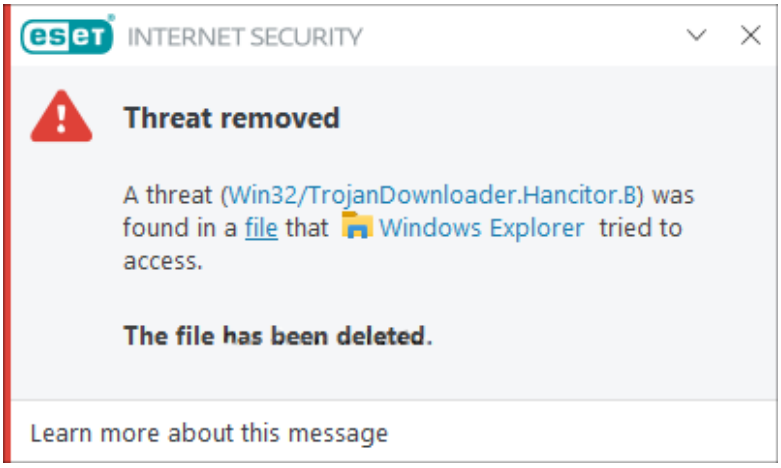
Security status alert

When we disabled real-time protection, an alert was shown on the home page (screenshot below) along with a Windows pop-up alert. We were able to reactivate the protection easily by clicking *Enable real-time file system protection*.



Malware detection alert

When a malicious file was detected in our functionality check, ESET displayed the alert shown below. We did not need to take any action. The alert closes after 10 seconds.



Clicking the threat name opened the according page of Virus Radar, ESET's online malware encyclopaedia, while *Learn more about this message* links to the product's online manual. The latter provides general information about threat detections and how to deal with them. When multiple malicious files were detected at the same time, ESET showed just one alert box. This allowed us to see threats one by one, using the *X* button, or to close all alerts at once using the drop-down menu in the top right-hand corner.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, an ESET pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. ESET immediately showed a detection alert, and deleted the malware samples on the drive within a couple of seconds, making it impossible to copy any of them to the test PC (or run an execution check). We would describe this as exemplary behaviour for a security program.

When we scanned the USB drive via Windows Explorer's right-click menu, ESET displayed the message *Scan completed: All detections cleaned*, and showed the number of detected items. There was an option to show the scan log. We consider this to be a good solution, as no user decision was required. All the malware samples were deleted from the USB drive.

Scan options

The *Computer scan* page allows you to start a complete system scan, drag and drop files for scanning, or start an advanced scan. The later allows you to create a custom scan, scan removable media scan, and repeat the last scan. Custom scan provides very granular options, including operating memory, boot sectors/UEFI, WMI database and registry. You can scan files and folders Windows File Explorer's right-click menu. Scanning for potentially unwanted (e.g. browser toolbars, trackware), potentially unsafe (e.g. hacker tools), and suspicious applications (e.g. those using typical malware obfuscation packing) can be enabled in *Setup|Advanced Setup|Protections*. Scan exceptions can be set in the *Exclusions* of the *Detection engine* section in the *Advanced Setup*.

Quarantine

The *Quarantine* page can be found under the *Tools* menu (in last year's review we suggested it would be easier to find there and are happy to see this change implemented). There you can see the date and time of detection, file name and path, file size, detection name, number of occurrences, the name of the active user at the time, and the SHA-1 hash of the file. Multiple quarantined files can only be selected by using keyboard shortcuts, which may not be intuitive to casual users. Similarly, there is no direct way to empty the quarantine as selected files can only be deleted from quarantine and restored by right-clicking.

Logs

The *Logs* page is also available under the *Tools* menu. It provides records of detections, events (such as updates), and scan results, along with events relating to the program's other features, such as anti-spam and parental control.

Help

The *Help and support* page includes links to *Help page, Knowledgebase*, and *Technical Support*. Information about the licence and product is also displayed here. Clicking *Help page* opens an online manual, with topics such as *System requirements, Installation* and *Beginner's guide* in a menu column on the left-hand side of the page. Each page opens detailed explanations and instructions, along with annotated screenshots. In addition to this there is a question mark icon on most pages of the program, which opens the according help page; this is an excellent feature, as it eliminates searching for the corresponding page in the online help.

Access control

Standard Windows User accounts cannot disable protection features, or uninstall the program. This is as it should be, in our opinion. Additionally, you can password protect the settings (*Setup\Advanced setup\User interface\Access setup*). If this is set up, other users (even admins) can operate all the features of the program, but not change any settings or disable the protection in any way.

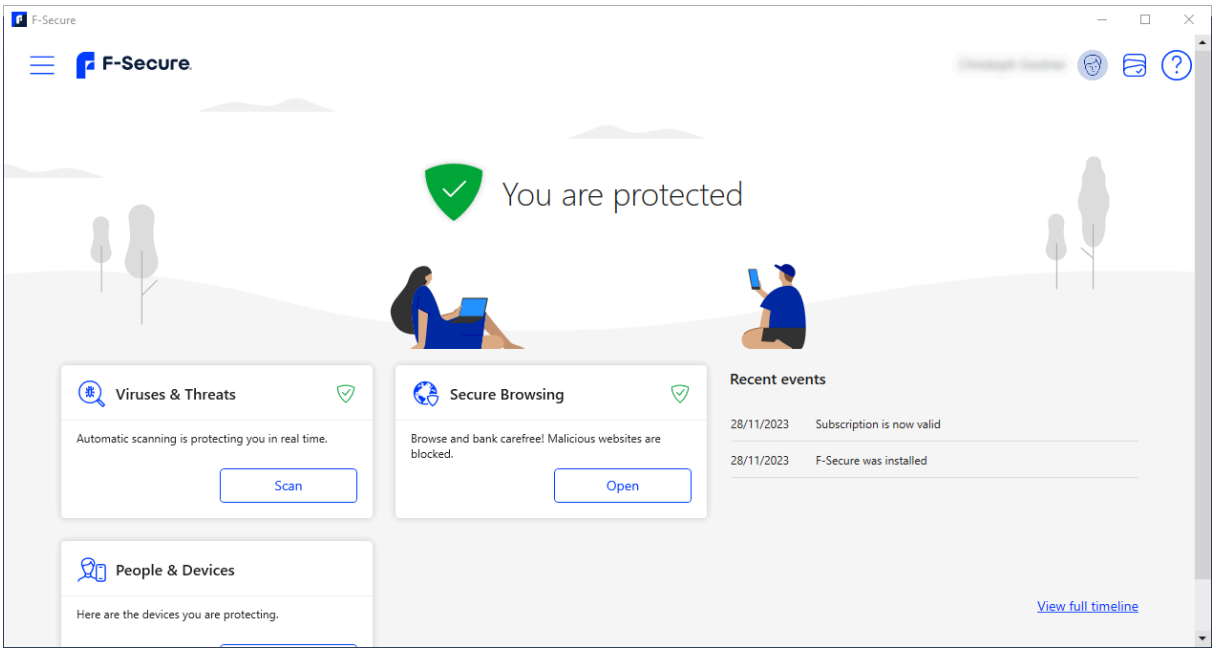
ESET Firewall

In our firewall check, the ESET Firewall worked perfectly. It continued to allow ping, file-sharing and Remote Desktop access to our test computer in our "home" network, but blocked all of these, and made the device invisible, when we connected to a "public" network. Should expert users nonetheless prefer to use Windows Firewall instead, it is possible to cleanly disable the ESET Firewall in the program's settings. This automatically enables Windows Firewall, without any warning messages being shown by either ESET or Windows Security. We consider this choice to be ideal.

Other points of interest

Under *Tools\More tools*, ESET provides a number of system utilities for advanced users, such as: *Running processes*, *Security report*, *Network connections*, and *System cleaner*. All of these could be useful for investigating suspicious behaviour on your system.

F-Secure Internet Security



About the program

F-Secure Internet Security is a paid-for security program with a sleek and visually pleasing design, which gives you quick access to all the features. It includes anti-malware and secure browsing features. The browser plug-ins add browsing and banking protection, as well as an ad blocker (which were not part of the functionality check). You can find out more about the program on the vendor's website: https://www.f-secure.com/en/internet-security

Summary

Installing the program is very straightforward, and the program's simple interface is easy to navigate and offers helpful explanations of all the included features. F-Secure Internet Security's handling of malware on external drives and network shares was outstanding in our functionality check.

Setup

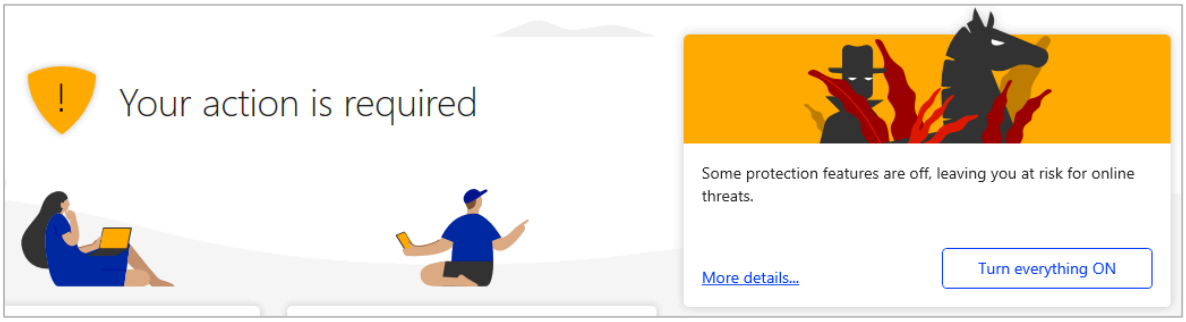
When downloading the installer, you have to select whether you are installing the program on your own device, you child's device, or the device of someone else (for this review we selected *My Device*). The installer allows you to select the language for the installer, and you can opt into sending usage data. There are no further steps necessary, and F-Secure launches automatically when the installation is finished. At this point, you can again select who you want to set up the program for. The program prompts you to install the browser add-ons for secure browsing, this is optional, however.

System Tray icon

The system tray icon can be used to open the program, check for updates, open the settings, view recent events, and see program information.

Security status alert

When we disabled protection features in the settings, an alert was shown on the home page (screenshot below), along with a Windows pop-up alert. We were easily able to reactivate all protection by clicking *Turn everything ON*.



Malware detection alert

When we opened a folder containing malicious files in our functionality check, F-Secure immediately quarantined all of the files and displayed the alert shown below. No further action was needed. The alert disappeared after 5 seconds.

When multiple malicious files were detected at the same time, F-Secure showed an alert for each of them. Clicking on the alert opened the Event history.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, an F-Secure pop-up alert invited us to scan the device for threats. We declined to run a scan, and opened the drive in Windows File Explorer. F-Secure immediately showed a detection alert, and deleted the malware samples on the drive within a couple of seconds, making it impossible to copy any of them to the test PC (or run an execution check). We would describe this as exemplary behaviour for a security program.

When we scanned the USB drive via Windows Explorer's right-click menu, F-Secure showed us a list of *Harmful items* found. The default action for each detected file – which can be changed on an individual basis – was set to *Clean Up*. We just had to click *Handle All*, and shortly afterwards, F-Secure informed us that *All harmful items were cleaned*. There was an option to *View scanning report*, and all the malware samples were deleted from the USB drive.

When we opened a writeable network share containing malware samples and clean files, F-Secure displayed a detection alert and deleted the source malware samples from the shared folder within a couple of seconds, so that we were not able to copy them to the Desktop. We find this to be outstanding.

Scan options

The *Scan* button at the bottom of the program window runs a quick scan of the computer. When you open the *Viruses & Threats* section you can run a full computer scan. Under *Settings\Scanning settings*, you can set up scheduled scans.

Quarantine

The quarantine is found under *App and file control* in the *Viruses & Threats* area; administrator privileges are needed to open this window. Here you can view quarantined, blocked, excluded, and protected (from ransomware) files, folders and programs. The quarantine shows the date and time of detection, the file name, and the infection name. Clicking on the latter opens a threat description on F-Secure's website. Clicking on an item shows the original file path, and allows you to set an exception, delete the file permanently, or report it as a false positive. Multiple quarantined files can only be selected by using keyboard shortcuts, which may not be intuitive to casual users.

Logs

Recent events are displayed on the program's home page, and respectively in the sections *Viruses & Threats* and *Secure Browsing*. There you can click on *Show full timeline* to show all applicable events that have taken place. Administrator rights are needed to clear or show all events.

Help

Clicking on the ? button on the start page allows you to open the product help; unlike most other products reviewed, the help feature is part of the program and therefore also available offline. Clicking the *?* symbol anywhere else in the app opens the help page for the open product feature. The help page is mostly text based, with the exception of images of certain buttons.

Access control

Standard Windows User accounts cannot disable protection features, or uninstall the program. This is as it should be, in our opinion. Additionally, editing most settings requires you to open the configuration page with administrator privileges. This extra step might be frustrating when frequently changing settings, but also prevents accidental changes.

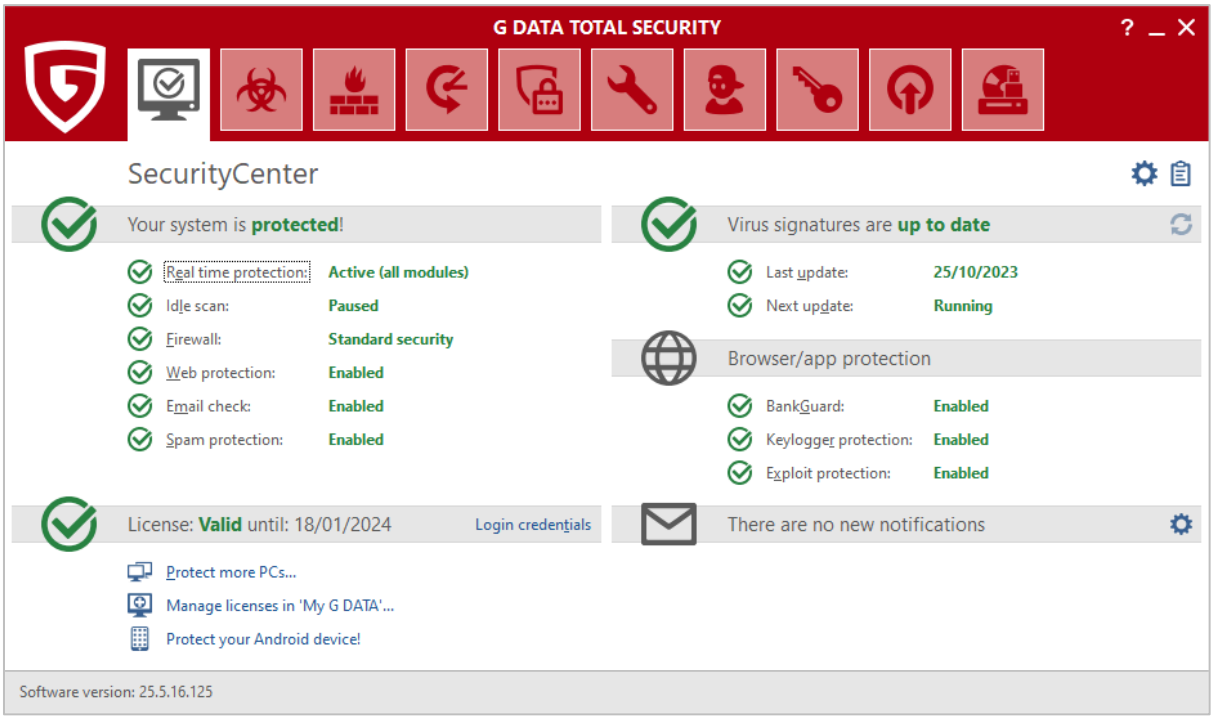
F-Secure Firewall

The product does not include its own firewall but links to the Windows Firewall settings from the *Viruses & Threats* section.

Other points of interest

- When opening a feature for the first time, you are shown a brief description of what it does.
- If you have a license for multiple users and devices, you can see the protection status of the other users in the *People & Devices* section.

G Data Total Security



About the program

In addition to anti-malware features, it includes anti-spam and anti-phishing components, a replacement firewall, backup function, encryption manager, password manager, device control, performance tuner, and parental controls. You can find out more about the program on the vendor's website: https://www.gdatasoftware.com/total-security

Summary

The interface of G Data Total Security is easily navigated, via a single row of tiles. There is a choice of a default or a customised installation, whereby the latter lets you choose individual components to install. The status display provides details of individual protection components, and access control is excellent. Most commendably, USB devices are proactively scanned for malware on connection. On-access protection means that files are scanned for malware if you try to copy them to your PC.

Setup

The setup wizard starts by asking you which interface language you would like to use. There is then a choice of *Standard* or *User-Defined Installation*. The latter lets you choose which optional components, such as anti-spam and parental controls, to install. You can also change the installation folder. At the end of the wizard, you can activate the full license with a registration key or login credentials. You can also opt for the 30-day trial. You need to restart your computer to finish the installation.

System Tray icon

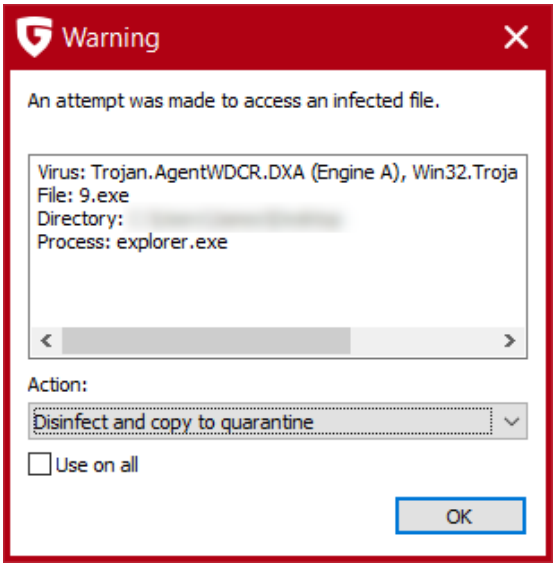
The System Tray icon menu lets you open the program window, disable malware protection, disable the G Data firewall, disable *Autopilot*, run updates, and see protection statistics.

Security status alert

When we disabled real-time protection in the program's settings, G Data displayed the alert below in the program window. We were able to reactivate protection by clicking *Real time protection\Enable virus monitor*.

Malware detection alert

When a malicious file was detected in our functionality check, G Data displayed the alert shown below. We just needed to click *OK* to quarantine the malware. Other options are *Block file access*, *Move to Quarantine*, and *Delete*. The alert turned slightly transparent after a few second but persisted until we closed it.



When multiple malicious files were detected at the same time, G Data showed one alert box for each of them. However, selecting the *Use on all* checkbox applied the same action to all malware detections, without showing further alerts.

Malware detection scenarios

We performed an Execution Check with G Data, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, a G Data detection alert was shown. Almost simultaneously, a G Data pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. We saw that G Data had already begun to delete the malware samples. When we copied the drive's remaining contents to the Windows Desktop, none of the malware samples was copied, and we found that all the source malware files had been deleted from the USB drive. We regard this as excellent.

When we scanned the USB drive via Windows Explorer's right-click menu, we noted that G Data had proactively detected and deleted the malware samples on the root of the drive before we were able to start the scan, and without our opening the drive in Explorer. We regard this as commendable. The on-demand scan thus only detected the malware samples in the drive's subfolder. At the end of the scan, G Data showed us a list of the malicious files found, including the file names and paths, with the default action set to *Disinfect and copy to quarantine* for all of them. We then just had to click *Execute actions*. All the malware samples were deleted from the USB drive.

When we copied some malware samples and clean files from a network share to the Windows Desktop of our test PC, G Data displayed a detection alert, prompting us to take action. The default action was set to *Disinfect and copy to quarantine*. All of the malware samples were copied to the Desktop; it was not until we clicked *OK* on the detection prompt that G Data deleted them.

Scan options

The *Virus protection* page (second icon from left on the top toolbar) provides a number of different scan options. These are: *Check computer (all local drives); Scheduled virus checks; Check memory and Autostart; Check directories and files; check removeable media; Check for rootkits*. You can also scan a local drive, folder or file, or network share, using Windows File Explorer's right-click menu. Scan options in the *Anti-Virus* section of the *Settings* dialog let you choose which protection components should be used (all are on by default). You can also choose whether to detect potentially unwanted programs (on by default). Exceptions for both real-time protection and on-demand scans can be set here too.

Quarantine

The quarantine function can be opened from the *Anti-Virus* page. It shows the date and time of detection, threat name, file name and path. You can disinfect, delete or restore files one at a time, or use standard Windows keyboard shortcuts to select multiple items, which may not be intuitive to casual users.

Logs

Logs can be opened from the clipboard icon in the top right-hand corner of the window. You can see details of scans, detections and signature updates. Clicking on any item displays a details pane below with applicable information about the event in question, such as program and signature versions, protection components used, and areas scanned. You can view all logs or only show logs related to *Updates, Real-Time Protection, Virus Scans,* or *Web & Mail*.

Help

G Data 's online help pages can be opened by clicking the question-mark icon in the top right-hand corner of the window or pressing F1. Thia opens the online documentation for the G Data Security Center. There are several categories listed here, such as *Overarching Features, Real-time protection, Idle scan*, or *Firewall* among others. For each item, there is a very detailed page of instructions and explanations, very well illustrated with screenshots.

Access control

Standard Windows User accounts cannot disable protection features or uninstall the program, which we regard as ideal. You can also password protect the settings, to prevent any other users changing them.

G Data Firewall

As noted in previous years' reports, the G Data firewall automatically sets all wireless networks to Trusted (equivalent to Windows' Private setting), overriding Windows (which sets them to Public by default). Hence, when we connected to our "public" network, G Data treated it as Private, and so we were able to see the test PC's hostname, IPv4 address and MAC address, as well as being able to open its file share, and a document contained within it. Only when we proactively went into G Data's firewall settings and set the wireless network adapter to Untrusted (Public) was the test PC hidden and protected on the "public" network. In our opinion, this exposes G Data users to unnecessary risk when using public networks, a problem that could easily be solved by setting all wireless networks to Public by default (as Windows does).

Other points of interest

- After installation, we were prompted to install the G Data add-on for Google Chrome.
- On the *Virus protection* page, under *Boot medium*, you can create a bootable CD/DVD/USB drive that you can use to scan an already-infected PC.

K7 Total Security

About the program

K7 Total Security is a paid-for security program. In addition to anti-malware features, it includes a parental control feature, which allows for whitelist/blacklist web filtering and Internet time restrictions. There is also an anti-spam feature, a replacement firewall, tune-up function, device control, and secure delete feature. You can find out more about the product on the vendor's website: https://k7computing.com/us/home-users/total-security

Summary

We found K7 Total Security to be very simple to install and use. The most important functions can easily be accessed from the home page. The default actions for connecting external drives and malware detection are ideal. In our functionality check, K7's highly sensitive on-access protection detected and removed malware on USB drives and network shares as soon as they were opened in Windows File Explorer. Access control is excellent.

Setup

Installation is extremely quick and simple. Having started the installer file, you just need to click *Install*, and less than a minute later the program is up and running. At the end of the wizard, you are asked to supply your login credentials, and enter a licence key to activate the program. There is also a prompt to install the K7 browser extension for Chrome.

System Tray icon

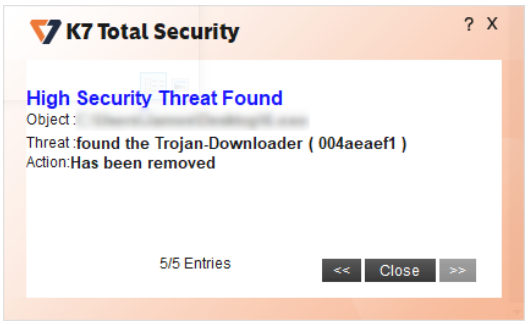
The System Tray menu lets you open the program, run scans and updates, disable/enable protection, halt network traffic, enable gaming mode, see product information, and access help features.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Fix Now*.

Malware detection alert

When a malicious file was detected in our functionality check, K7 displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds.



When multiple malicious files were detected at the same time, K7 showed just one alert box, which allowed us to browse through the various threats to see details, and to close all alerts.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, a K7 pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. K7 immediately showed a detection alert, and deleted the malware samples on the drive within a couple of seconds, making it impossible to copy any of them to the test PC (or run an execution check). We would describe this as exemplary behaviour for a security program.

When we scanned the USB drive via Windows Explorer's right-click menu, K7 displayed the message *Scan Completed*. All security risks were removed successfully. The dialog box showed the path and filenames of the detected items, along with a description of the malware type, and the action taken. We consider this to be an optimal solution, as no user decision was required, and file names/locations were shown up front. All the malware samples were deleted from the USB drive.

When we opened a writeable network share containing malware samples and clean files, K7 displayed a detection alert and deleted the source malware samples from the shared folder within a couple of seconds, so that we were not able to copy them to the Desktop. We find this to be outstanding.

Scan options

Pressing the *Scan* button at the bottom of the program window lets you run quick, complete, custom, or rootkit scans, and set scheduled scans. Local drives, folders files, or a network share can be scanned using Windows Explorer's right-click menu. Under *Settings\Antivirus and Antispyware*, you can choose whether to scan for *Spyware and Adware* (on by default), and set scan exclusions. From here it is also possible to change the default action on detection.

Quarantine

The quarantine is found under *Reports\Quarantine Manager*. From here, you can delete or restore detected malware items, view their properties, and add items to the quarantine. The page shows date and time of detection, file name and path, malware type, and file hash. Multiple quarantined files can only be selected by using keyboard shortcuts, which may not be intuitive to casual users.

Logs

You can find the logs feature under *Reports\Security History*. There are separate logs for antivirus, firewall, and privacy.

Help

Clicking on *Help* in the top right-hand corner of the window opens a local help file. This lists a variety of topics, covering the configuration and use of the product. Simple, clear instructions are provided for each topic, some illustrated with screenshots.

Access control

By default, standard Windows users are not able to disable protection features, or uninstall the program. This is as it should be, in our opinion. Under *Settings\General Settings*, you can set a password that all users have to enter in order to disable protection. Here you can also allow non-administrator users to change settings and disable protection.

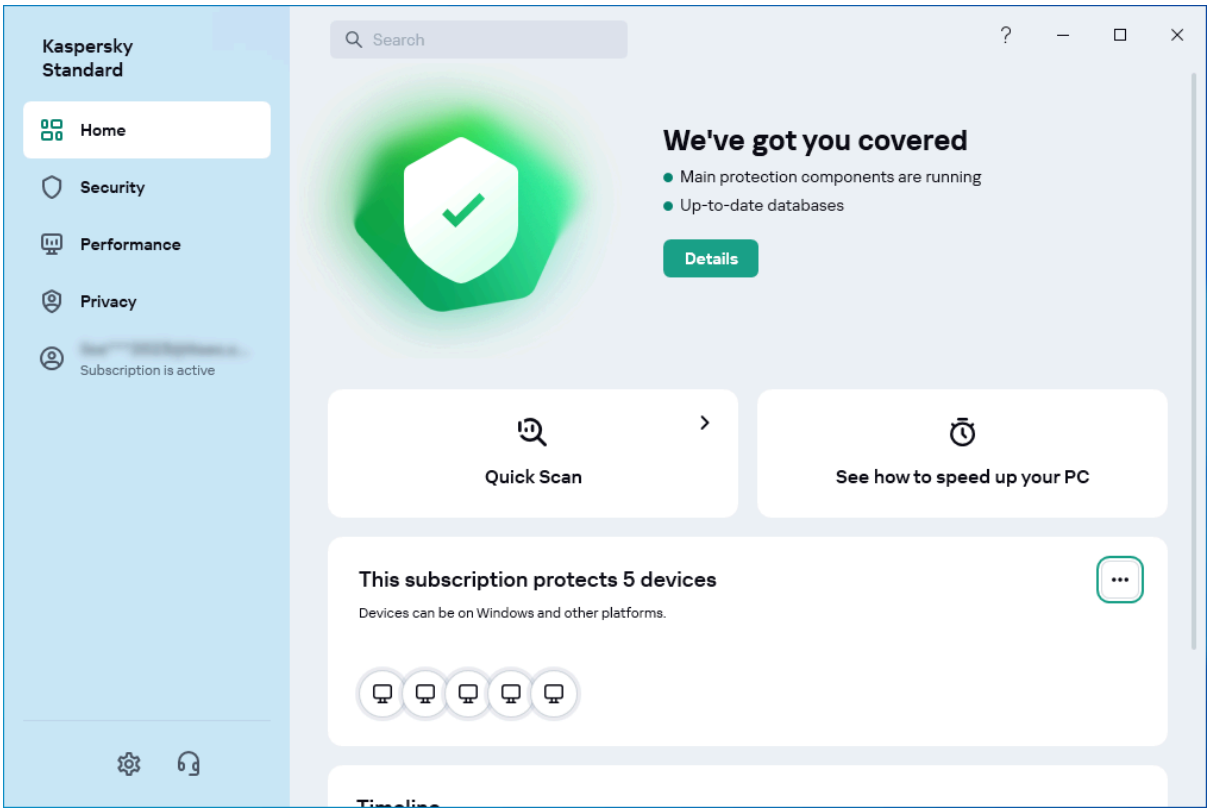
K7 Firewall

In our firewall check, K7 performed mostly as expected, but with one significant flaw. When we connected our "public" network, we found that K7 blocked ping requests and Remote Desktop connections, and made the shared folder inaccessible. However, we were able to see the device's hostname, MAC address and IPv4 address from another computer in the network (representing a hacker's PC in e.g. a hotel WLAN), using Windows Explorer's Network view. We feel that this is a significant security issue that the vendor should correct as soon as possible.

Other points of interest

- K7's application-control and ad-blocking functionality can be found in the *Parental Control* section of the settings.
- The program's additional features include *Computer TuneUp* and *Secure Delete*, this can all be found in the *Tools* section.
- Throughout the year, we were inundated with frequent emails from K7 urging us to renew a long-expired subscription. These emails arrived monthly, sometimes bombarding us with up to half a dozen per day. They often falsely claimed to be from "*Windows Security*" or bore subjects like "*Security Alert*" or "*Thank you for choosing to remain with K7*." Furthermore, many lacked an unsubscribe link, and even if included, it was ineffective/non-functional. This behavior resembled spam rather than that of a reputable vendor. Upon alerting K7 to this issue initially, they assured us it was resolved, resulting in a temporary cessation of emails. However, after a few weeks, the messages resumed. Upon escalation to K7's management, we appreciate the prompt attention given to address this matter, caused by an external company. The issue has since been resolved. While we understand the challenges in customer retention, the unprecedented and persistent frequency of these messages became increasingly disruptive and frustrating.

Kaspersky Standard



About the program

Kaspersky Standard is a paid-for security program that includes various anti-malware functions, as well as a vulnerability scanner, software updater, ransomware protection, added protection for banking and financial websites, webcam protection, and browser privacy features. You can find out more about the product on the vendor's website: https://kaspersky.com/standard

Summary

Installation of Kaspersky Standard is straightforward, with safe default options. The program's modern, tiled interface makes all essential features easily accessible from the home page. In our functionality check, Kaspersky's highly sensitive on-access protection proactively deleted malware on a network share as soon as we opened it in Windows File Explorer, the same thing occurred when opening network shares. Advanced users will find a wide range of configuration options in the settings.

Setup

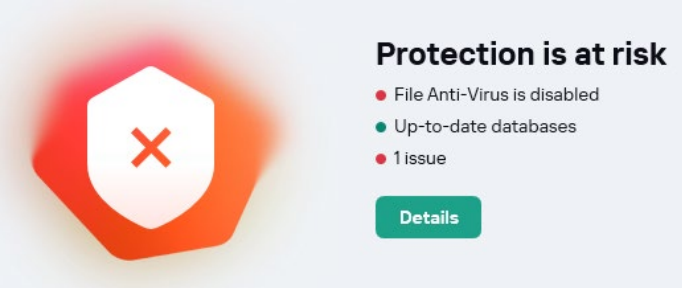
The installer lets you opt out of participating in the *Kaspersky Security Network* (on by default). Then you just have to click *Continue* to start setup. After restarting, the installation finishes and you are guided through the rest of the setup process in a chat-style interface. You are taken through activating the product, asked if an initial scan should be run, and introduced to the product's other features; at all times you have the option to skip this introduction. The entire process is very smooth and intuitive.

System Tray icon

The System Tray icon menu lets you open the program, pause and resume protection, open settings, view the support page, see program information, or exit the program.

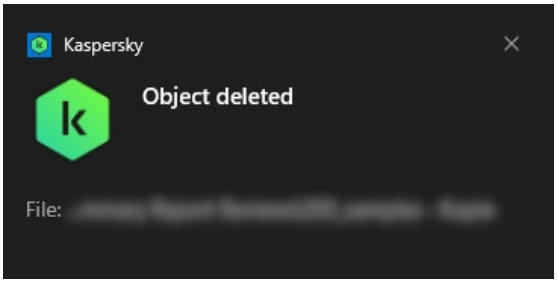
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below) along with a Windows pop-up alert. We were able to reactivate the protection easily by clicking *Details*, then *Enable*.



Malware detection alert

When a malicious file was detected in our functionality check, Kaspersky displayed the message box shown below. We did not need to take any action. The alert closed after 10 seconds.



Clicking on the alert opened the logs page with additional information on the detection. When multiple malicious files were detected at the same time, Kaspersky displayed one alert box for each detection.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, Kaspersky did not initially take any action. When we then opened the drive in Windows File Explorer, Kaspersky showed a detection alert, and deleted the malware samples on the drive within about 10 seconds. Consequently, we did not have enough time to copy them to the test PC (or run an execution check). We would describe this as excellent behaviour for a security program.

When we scanned the USB drive via Windows Explorer's right-click menu, Kaspersky displayed the message 1 object disinfected, 9 objects deleted. There was an option to show a Detailed report. We consider this to be a good solution, as no user decision was required. Whilst the notification 1 object disinfected was technically incorrect, the action taken was entirely appropriate. All the malware samples were deleted from the USB drive. When we opened a writeable network share containing malware samples and clean files, Kaspersky displayed a detection alert, and deleted the source malware samples from the shared folder in the space of about 10 seconds. We were thus not able to copy them to the Desktop. We find this to be excellent.

Scan options

Clicking the arrow on the *Quick Scan* tile or under *Security\Choose scan* opens the *Scan* page. The button on the program's home page opens the *Scan* page. You can run a *Quick Scan*, a *Full* Scan, a *Selective Scan*, a *Removable Drive Scan*, or an *Application Vulnerability Scan*.

All of these can be scheduled, by clicking the cogwheel icon next to the scan. A local drive, folder or file, or a network share can be scanned from Windows Explorer's right-click menu. To manage scan exclusions, you have to open the *Security settings* in the settings (cogwheel icon in the bottom left-hand corner of the window) and then go to *Exclusions and actions on object detection* at the very bottom of the page. You can specify which protection components – e.g. real-time protection, on-demand scans – the exclusion should be applied to. *Adware* and *Auto-dialers* detection is on by default and cannot be disabled, other PUA detection is toggled with the *Unwanted App Installation Blocker* switch in the Privacy section.

Quarantine

The quarantine feature can be found by clicking *Security\Quarantine*. It shows the file name and path, detection name and date/time of detection, and the action taken. You can select files individually or all at once. Files can be deleted or restored, and you can open the folder where the file was detected.

Logs

The log function can be opened by clicking *Security \Reports*. A wide variety of reports is provided, including individual reports for the different protection components, such as *File Anti-Virus, Web Anti-Virus*, *Firewall, and* for additional features, such as *Anti-Spam* and *Software Updater*. The reports can be filtered by time period and relevance.

Help

The question-mark symbol in the top right-hand corner of the window opens Kaspersky's online manual for the current page of the program. Straightforward text-only instructions for each feature are provided. A left-hand menu column lets you navigate easily to other topics.

Access control

Standard Windows users have full control of the program's settings and can disable protection features. However, only users with administrator accounts can uninstall the program. You can password protect the program. All users then have to enter the password to access settings or disable protection by any means. You also have the option to only block access to certain settings.

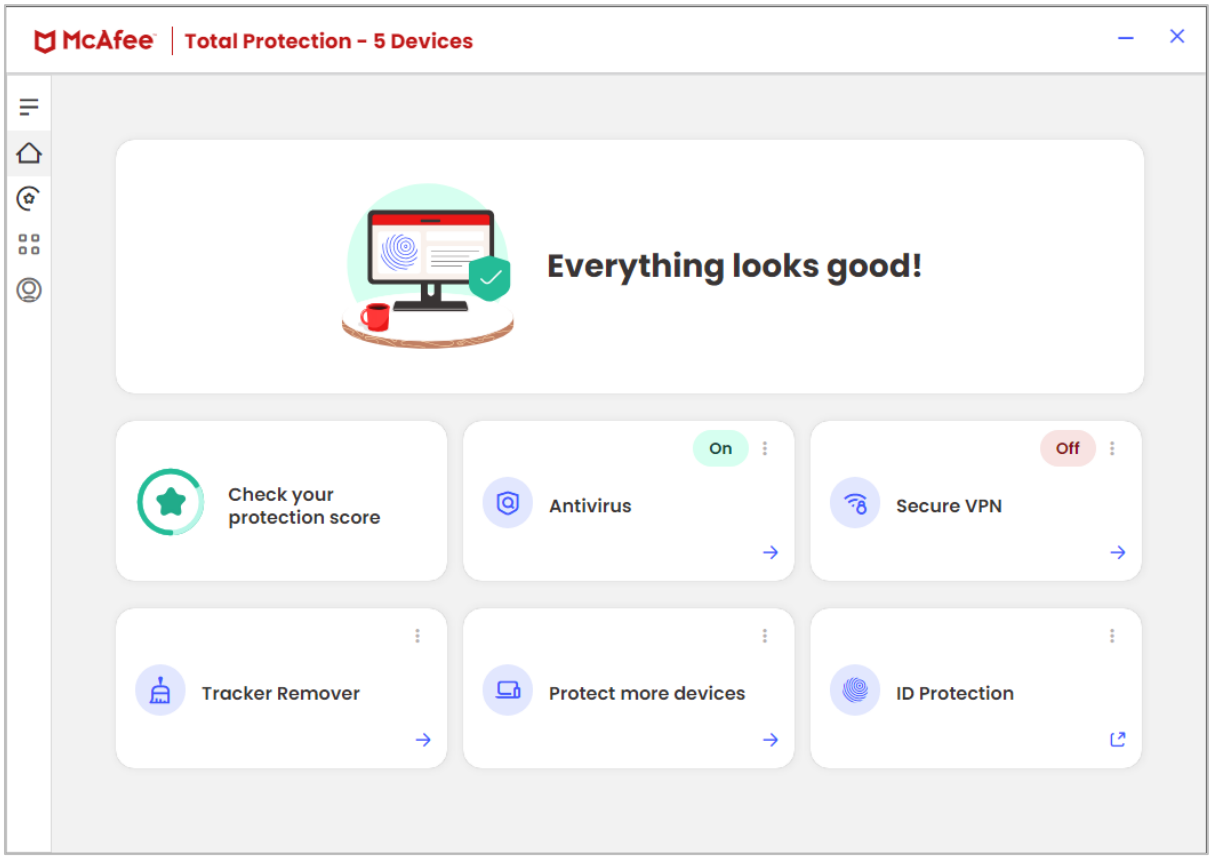
Kaspersky Firewall

In our firewall check, Kaspersky did not prevent discovery of our test device in the "public" network. This meant that we were able to see its hostname, IPv4 address and MAC address from another computer in the same public network (representing a hacker's PC in e.g. a hotel WLAN), using Windows Explorer's Network view. We were also able to establish a Remote Desktop connection to the device. Kaspersky tell us that they are investigating this issue and plan to rectify it in a future build.

Other points of interest:

- The search bar at the top of the program can be used to find features and settings.
- Scan settings can be found by clicking the *Scan* tile on the homepage, not under *Settings*.
- The *Security\Weak Settings Scan* can search for settings that might put your device at risk.
- There are several options to improve system performance available in the *Performance* section. These were not part of our functionality check.

McAfee Total Protection



About the program

McAfee Total Protection is a paid-for security program. In addition to anti-malware features, it includes a VPN, password manager, replacement firewall, cookie and tracker remover, and secure file-deletion feature. You can find out more about McAfee Total Protection on the vendor's website: https://www.mcafee.com/en-us/antivirus/mcafee-total-protection.html

Summary

McAfee Total Protection is very simple to install, and has a modern, touch-friendly interface. The essential functions can be accessed via tiles on the home screen, and the malware alerts are clear and persistent. and the McAfee Firewall co-ordinates perfectly with Windows' network settings.

Setup

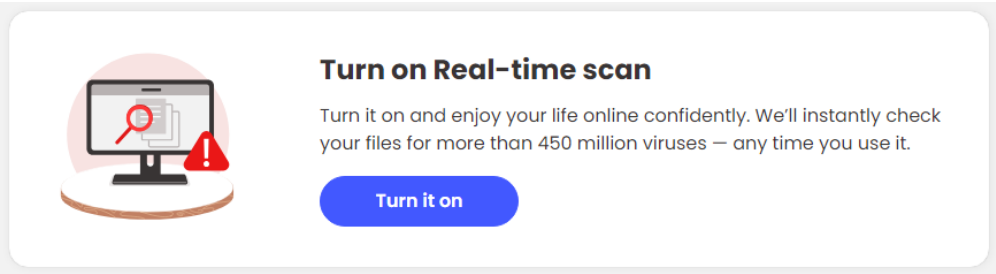
McAfee has one of the most straightforward installations. You only have to click *Install*, and that's it. The program window opens automatically after installation finishes.

System Tray icon

The System Tray icon menu lets you open the program window, check for updates, run scans, access settings, turn on the VPN, view subscription information and your account, as well as open the help page.

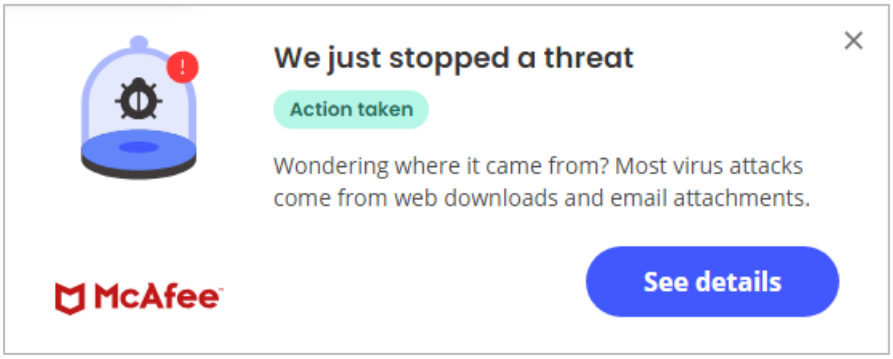
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below) and there was a pop-up notification, which persisted until we closed it. We were able to reactivate the protection easily by clicking *Turn it on*.



Malware detection alert

When we tried to open a malicious file in our functionality check, McAfee blocked this and displayed the alert shown below. We did not need to take any action, and the alert persisted until we closed it.



Clicking *See details* displayed the file name and path, detection name, and action taken (*Quarantined*).

Malware detection scenarios

We performed an Execution Check with McAfee, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, a McAfee pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and instead opened the drive in Windows Explorer. We were able to copy all the files from the drive to the Windows Desktop without McAfee reacting. However, as noted above, the malware samples would have been instantly detected had we tried to execute them.

When we scanned the USB drive via Windows Explorer's right-click menu, McAfee displayed the message We resolved 10 threats – you're protected. There was an option to See details. We feel this is in itself a good solution, as no user decision was required. However, when we checked the USB drive after performing the scan, we found that four out of the five malware samples in the drive's subfolder (duplicates of the five samples on the root of the drive) had been deleted, while the remaining one, plus the five samples on the drive root, had not. Although all the remaining six malware samples had in fact been rendered completely harmless, we found McAfee's behaviour here to be confusing. We suggest that simply deleting all malicious files would be a better option.

Scan options

Click the *Antivirus* tile on the home page, allows you to run a quick or full scan and to schedule scans. You can also scan a local drive, folder or file, or a network share, from Windows Explorer's right-click menu. Clicking the *My Protection* icon (icon with four squares on the left-hand side of the program window), then *Real-Time Scanning,* allowed us to exclude individual files from being scanned. We could not find settings for PUA detection.

Quarantine

This is found under *My Protection\Quarantined items*. The quarantine shows the file name, threat name, and date/time of detection and status. Clicking on items displays the original file path. You can restore or delete individual items, or all items together with the *Select all* button.

Logs

The log feature is found under *My Protection\Security Report*. This shows a record of things such as threats resolved, files scanned, and items quarantined. The results can be filtered for the last week, month, and year.

Help

The help features can be accessed by clicking the *Account* icon (at the bottom of the row of icons on the left-hand side). The *Help* link opens a web page from which you can contact McAfee customer services. The *Support Website* link opens the McAfee customer service page, which has links to customer support, a virtual assistant, and the community page. There is also search function available on the *Support Website*. Both of these pages appear similar, which could make finding instructions difficult, especially for novice users.

Access control

Standard Windows Users cannot disable protection features (the switches are deactivated), or uninstall the program. This is as it should be, in our opinion.

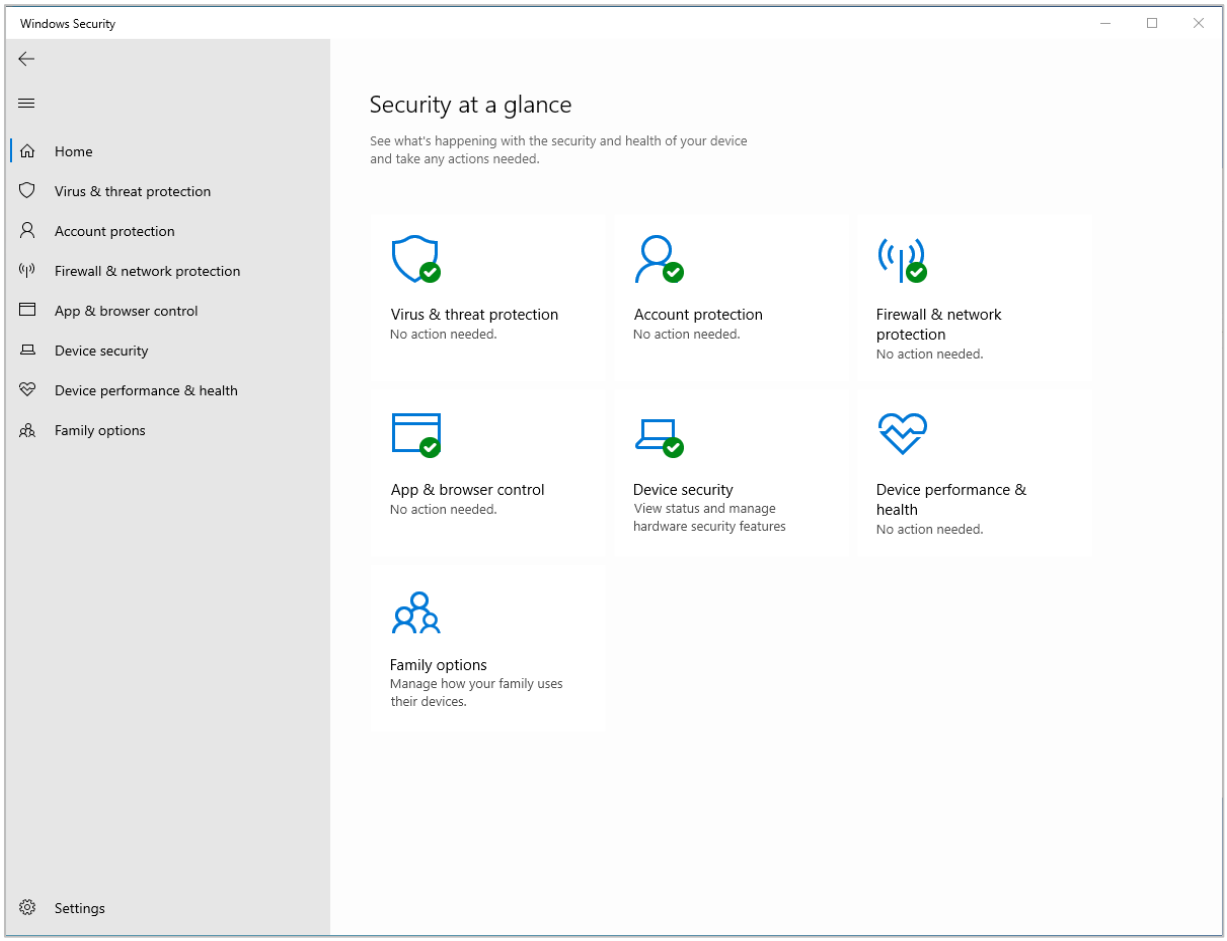
McAfee Firewall

In our firewall check, the McAfee Firewall worked perfectly. It continued to allow ping, file-sharing and Remote Desktop access to our test computer in our "home" network, but blocked all of these, and made the device invisible, when we connected to a "public" network.

Other points of interest:

- There is a VPN included, with a wide selection of countries.
- The McAfee WebAdvisor plugin can be added to your browser.
- The file shredder, which can be used to more securely delete files or folders, can also be accessed from the right-click menu in File Explorer.

Microsoft Defender Antivirus



About the program

Microsoft Defender Antivirus is a free security program, included with Windows 10 (and Windows 11). You can find out more about the program on the Microsoft website: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963

Summary

Microsoft Defender Antivirus includes all the essential features of an antivirus program in a clean, touch-friendly interface. The program is simple to use and comes pre-installed with Windows.

Setup

Setup is not required, as the program is built into Windows.

System Tray icon

The System Tray icon menu lets you run a quick scan, check for updates, view notification options, and open the Windows Security dashboard.

Malware detection alert

When a malicious file was detected in our functionality check, Microsoft Defender Antivirus displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds.

Clicking on *Get details* opened the *Virus & threat protection* page of Windows Security. When multiple malicious files were detected at the same time. An individual alert was shown for each detection.

Malware detection scenarios

We performed an Execution Check with Microsoft, which involved trying to run our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, Microsoft did not initially take any action. When we opened the drive in Windows File Explorer, Microsoft showed a detection alert, and began gradually deleting the malicious files from the USB device, which is commendable. We were able to copy some of the malware samples to the Windows Desktop, although these files were deleted after about 15 seconds.

When we scanned the USB drive via Windows Explorer's right-click menu, Microsoft displayed a list of the malware samples detected, along with the message *Threats found - Start the recommended actions*. We then just had to click *Start actions*, and shortly afterwards, Microsoft informed us that there were *No current threats*. There was an option to show *Protection history*. All the malware samples were deleted from the USB drive.

When we opened a writeable network share containing malware samples and clean files, Microsoft displayed a detection alert and started gradually deleting the source malicious files from the shared folder, which is commendable. We were able to copy some of the malware samples to the Desktop of the test PC; Microsoft deleted these about 30 seconds after the copy procedure had completed.

Scan options

Opening *Virus & threat protection* allows you to run a quick scan. By clicking on *Scan options*, you can choose between a quick scan, full scan, custom scan (you can select the files or folders to scan), and a *Microsoft Defender Offline scan*. The later can be used to remove more stubborn malware, involves the device restarting, and takes about 15 minutes. Local drives, folders, files, or networks shares can be scanned by using Windows Explorer's right-click menu. Exclusions can be set under *Virus & threat protection\Manage Settings*. PUA detection is on by default and can be configured under *App & browser control\Reputation-based protection settings*.

Quarantine

The quarantine function is found by going to *Virus and threat protection\Protection history* and then filtering for *Quarantined items* (in our opinion, this is not the easiest or most obvious way of accessing quarantine functionality). There quarantined items are listed with date and time of detection, and severity. Clicking an item shows more details, which include the file path and name, and a brief description of the threat and the action taken. Files in quarantine can only be individually restored or removed. Clicking *Learn more* opens the Microsoft Security Intelligence website with additional information on the threat.

Logs

The log feature is effectively combined with quarantine under *Protection history*.

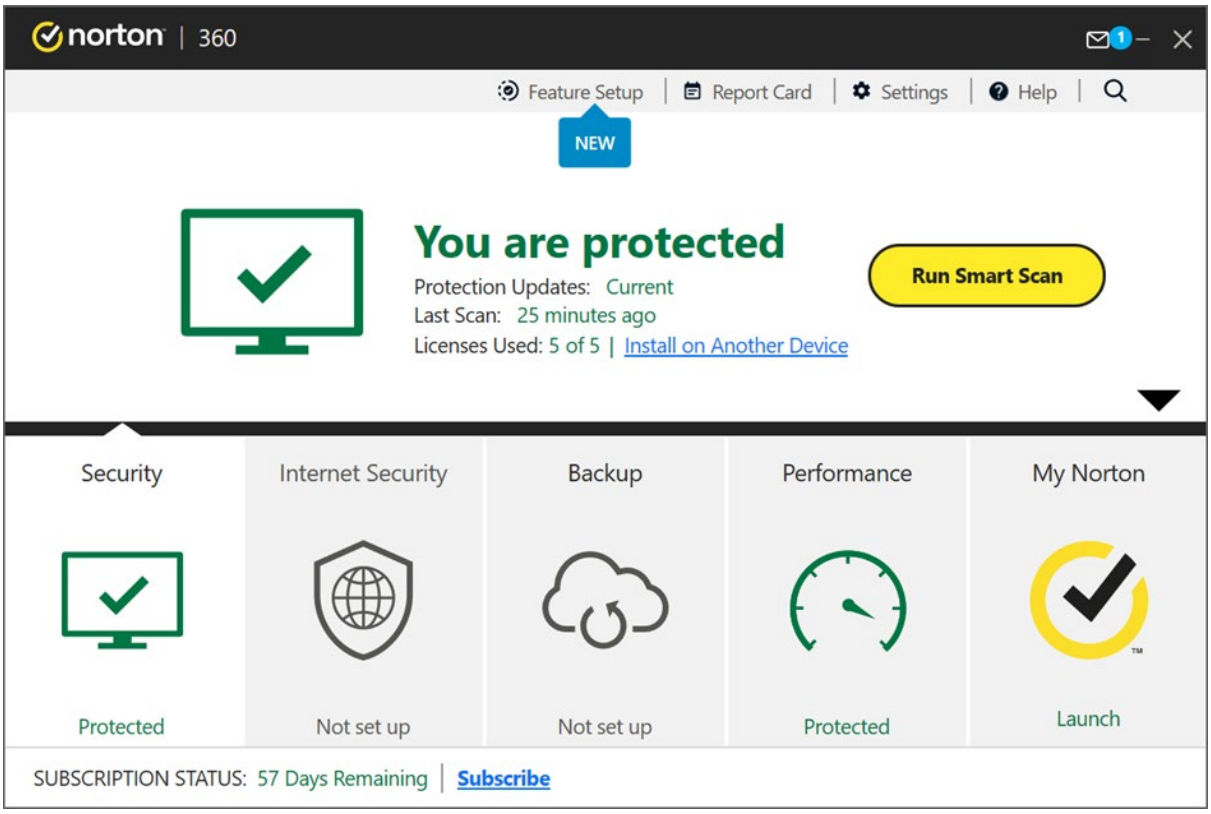
Help

Clicking *Get help* from the *Virus and threat protection* page opens the automated *Get Help* chat service. You can type in a query, and search. In our functionality check, we found the search not to be very helpful. For example, "Set scan exclusion" first shows information on how to use a scanner with your PC, before linking to the correct page under *More help*. This brought up a brief description illustrated with a screenshot.

Access control

Standard Windows User accounts cannot disable protection features, which is as it should be, in our opinion.

Norton AntiVirus Plus



About the program

Norton Antivirus Plus is a paid-for security program. In addition to anti-malware features, it includes a replacement firewall, cloud backup feature, password manager, software updater and performance tune-up features. You can find out more about the product on the vendor's website: https://us.norton.com/products/norton-360-antivirus-plus#

Summary

Norton 360 is very simple to set up, and has a very modern interface, where essential features are easy to find. Safe default settings are provided. On-access protection scans files when you try to copy them to your PC.

Setup

After logging into your Norton online account, you can download the installer. When running this, you can opt into Norton's data sharing scheme. After this, installation completes without the need for further intervention. When installation is finished, you can set up Cloud-Backup and Password Manager. After Norton starts for the first time, there is a brief tour of the program's features.

System Tray icon

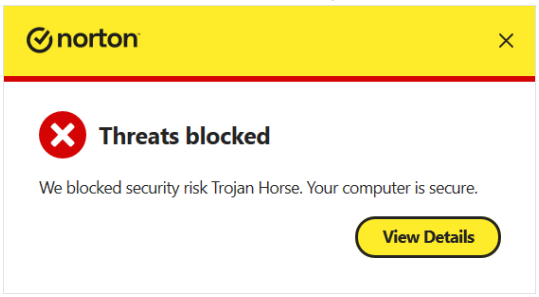
The System Tray menu lets you open the program, run scans and updates, access support, enable silent mode, disable antivirus and firewall features, open settings, and view logs.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below), and as a pop-up in the bottom right-hand corner of the screen. We could reactivate the protection easily by clicking *Fix Now*.

Malware detection alert

When a malicious file was detected in our functionality check, Norton displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds.



Malware detection scenarios

We performed an Execution Check with Norton, which involved trying to run our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process.

When we attached a USB flash drive with some malware samples and clean files to our test PC, a Norton pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. Norton immediately showed a detection alert, and gradually started deleting the malicious files on the drive, which is commendable. We attempted to copy the drive's contents (which still included most of the malware samples) to the Windows Desktop; Norton prevented any of the malicious files from being copied, which we find to be very good.

When we scanned the USB drive via Windows Explorer's right-click menu, Norton displayed the message All Threats Resolved, along with the detection names of the malware samples. There was also an option to see a *Results Summary*. We consider this to be a good solution, as no user decision was required. All the malware samples were deleted from the USB drive.

We were able to open a network share containing some malware samples and clean files, and copy the contents of the shared folder to the Windows Desktop, without Norton taking any immediate action. However, as noted above, the malware samples would have been instantly detected had we tried to execute them. About 30 seconds after the copy process had completed, Norton displayed a detection alert, and gradually deleted the copied malware files from the Desktop.

Scan options

The *Scans* button on the *Security* page opens a new window, where you can run smart, quick, full and custom scans, whereby a custom scan can be scheduled. Local drives, folders or files, and network shares can be scanned using Windows Explorer's right-click menu. The same menu can be used to check a file with Norton's reputation service. Exclusions are set under *Settings\Antivirus\Scans and Risks*. You can set exclusions and specify treatment of *Low Risks*, which we assume means PUAs.

Quarantine

This is found under *Security\History*; you can set the filter to only show quarantined items. This shows severity, what action was taken, the file name and detection name, and status, along with date and time of the detection. You have the option to search in the items listed. When you click on an item, more details are shown. These include a recommended action, and the ability to restore the file.

Logs

This is combined with the quarantine function.

Help

Clicking *Help* in the top right-hand corner of the window shows a number of help options, such as a link to the online help, and a diagnostics tool to checks to see that all components are functioning as intended. When changing settings, each group of settings has a *?* next to it; clicking this opens the corresponding support page.

Access control

Standard Windows users cannot disable protection features, or uninstall the program. This is as it should be. When the program is used by a user with a non-administrator account, protection settings are greyed out. There is also a password protection feature; when activated, the password is needed to change settings or disable protection.

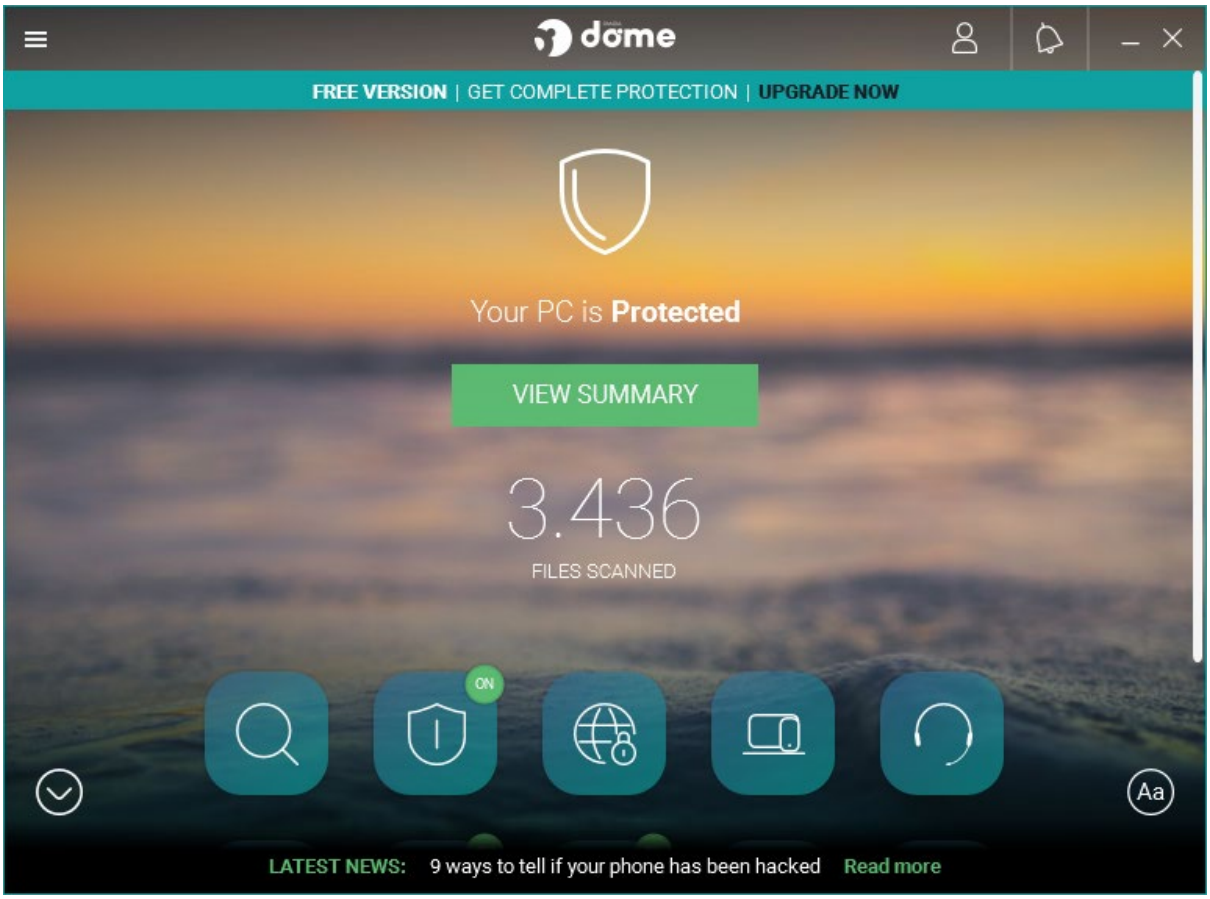
Norton Firewall

In our firewall check, the Norton Firewall worked perfectly. It continued to allow ping, file-sharing and Remote Desktop access to the test computer in our "home" network, but blocked all of these, and made the device invisible, when we connected to a "public" network."

Other points of interest

When we installed Norton on our test device, we encountered an issue where the program was installed in German despite the system language being English. A brief internet search indicated that we are not the only ones to face this issue.

Panda Free Antivirus



About the program

As the name suggests, Panda Free Antivirus is a free security program. In addition to anti-malware features, it also includes a limited VPN. You can find out more about the product on the vendor's website: https://www.pandasecurity.com/en/homeusers/solutions/free-antivirus/

Summary

We found Panda Free Antivirus to be very straightforward to install and use. The program interface is simple to navigate, and safe default options are provided. On-access protection means that files are scanned for malware when you copy them to your PC. The program window displays *LATEST NEWS* at the bottom of the window with security headlines, linking to Panda's security blog.

Setup

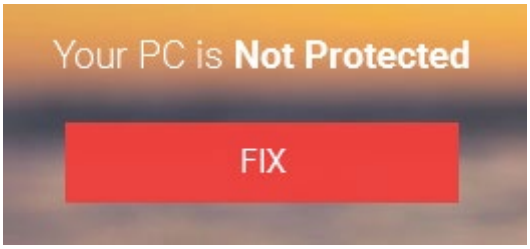
Installation is very straightforward. You can change the installation folder and interface language. By default, you are prompted to install the Opera browser, but you can easily opt out of this with a single click. In our functionality test, we did not install Opera. After the setup is complete, you are prompted to sign in or create a new Panda account. It is not essential to do this in order to use the program; however, if you don't, you will be prompted to sign in every time you open the program window.

System Tray icon

The System Tray icon menu lets you open the program window, enable gaming/multimedia mode, reach help and support services, disable/enable protection, and connect to the Panda VPN (which has limitations on servers and data).

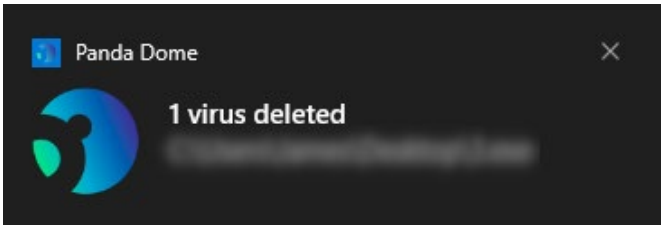
Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). After clicking *Fix*, and then *Enable*, protection was turned on again.



Malware detection alert

When a malicious file was detected in our functionality check, Panda displayed the alert below. We did not have to take any action, and the alert disappeared after a few seconds.



Clicking on this alert opened the *Event report* (logs) page, showing detection name, file name and path, date and time of detection, and action taken (deleted). When multiple malicious files were detected at the same time, individual notifications were displayed. However, these overlapped, so it appeared as if only one was displayed.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, a Panda pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. Panda did not take any action at this stage. When we copied the drive's contents to the Windows Desktop, Panda displayed an alert for each malicious file, in the form of a standard Windows pop-up. A few seconds after the copy process had completed, Panda began deleting the malware samples. When we scanned the USB drive via Windows Explorer's right-click menu, Panda informed us of the number of files scanned, and the number of detections. By clicking on Show details, we were able to see that Panda had "neutralized" the malware.

Scan options

Clicking the *Scan* button in the Panda app (magnifying-glass symbol) lets you run *Critical areas*, *Full, or Custom* scans. On the *Antivirus* page you can set scheduled scans, as well as view the last scan and quarantine. You can scan a local drive, folder or file using Windows Explorer's right-click menu. You can set exclusions and choose whether to detect PUAs (on by default) by opening *Settings\Antivirus* from the *Antivirus* page.

Quarantine

This feature is found on the *Antivirus* page. It shows you the detection name (along with the action taken), file name and path, plus date and time of detection. You can recover or delete quarantined items one by one, or empty the quarantine by clicking on the trash-can icon.

Logs

You can find the log feature on the *Antivirus* page, by clicking *View report*. It shows the same information as the quarantine page, along with the status (e.g. "Deleted").

Help

The help feature is located in the "hamburger" menu in the top left-hand corner of the window. Clicking on this opens an online manual for the product. The Support page can be reached by clicking on the support button on the start page of Pada Free Antivirus.

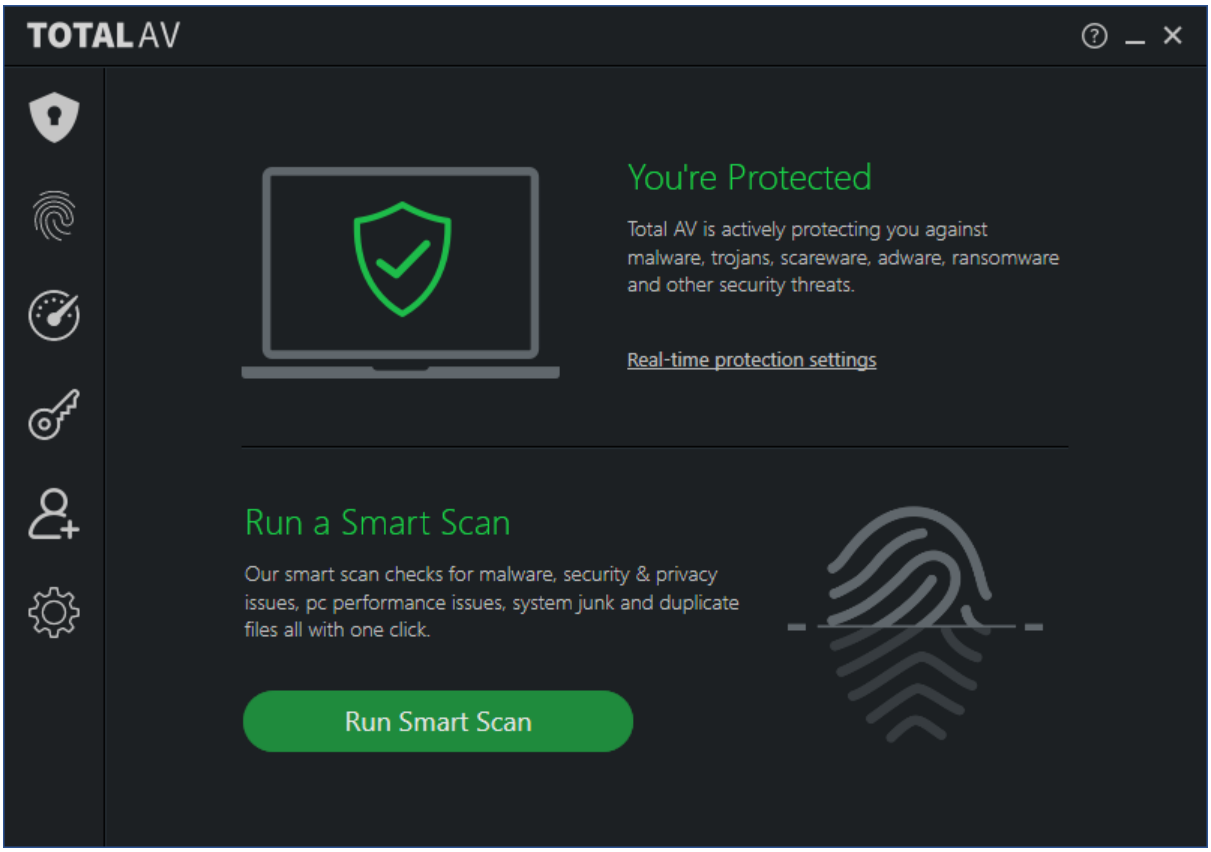
Access control

Standard Windows users can disable protection features, but not uninstall the program. You can however password protect the program. In this case, the password is required to access the Panda console. However, it will still be possible to run scans from Windows File Explorer's right-click menu, and see the results of this.

Other points of interest

- The setup wizard states that free support is included for "any PC or Internet related problems". UK, USA and Canadian telephone numbers are provided (in the English version of the program); Panda tell us that the calls are free of charge.
- The "Aa" symbol in the bottom right-hand corner of the window lets you show or hide the names of the symbols on the home page.
- The program's settings are found in the "hamburger" menu in the top left-had corner of the program window.
- A strip along the bottom of the windows displays headlines from Panda's Media Center. You can click on this to read the full story, and others. There are articles on various IT-security related topics.
- Although Panda Free Antivirus promotes other, paid-for Panda products, this is mostly done in a very subtle, non-intrusive way, by means of a thin strip along the top of the window.

TotalAV Antivirus Pro



About the program

TotalAV Antivirus Pro is a paid-for security program. In addition to anti-malware features, it includes phishing protection and a system performance tuner. You can find out more about TotalAV Antivirus Pro on the vendor's website: https://www.totalav.com/product/antivirus-pro

Summary

We found TotalAV Antivirus Pro to be very simple to install and use. The program's features are easily found in a single menu panel, and default settings and alerts are sensible. Files are scanned for malware if you try to copy them to your PC, and malware on a USB drive is detected as soon as you open the drive in Windows Explorer. The program also includes a VPN, although we did not test this.

Setup

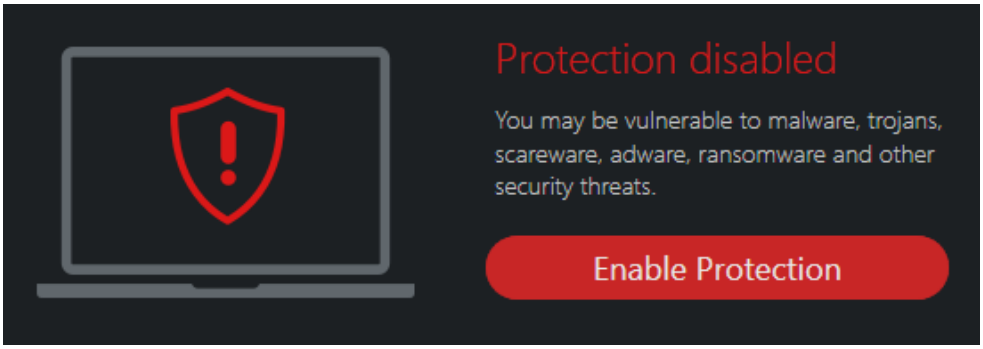
Installation is extremely quick and simple. All you need to do is run the installer, then click *Install*. After installing, TotalAV opens automatically and downloads definition updates.

System Tray icon

This lets you open the program window, open the settings, check for updates, and see information about program and definitions versions.

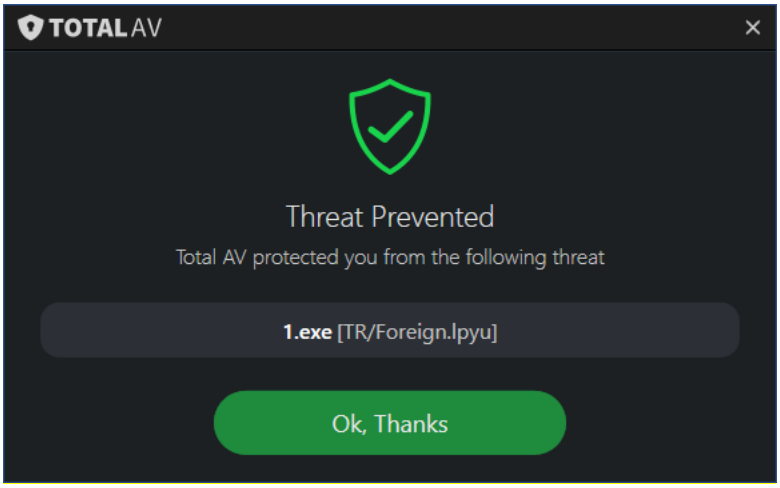
Security status alert

When we disabled real-time protection from the real-time protection settings, an alert was shown on the home page (screenshot below). Clicking *Enable Protection* reactivated protection.



Malware detection alert

When a malicious file was detected in our functionality check, TotalAV displayed the alert shown below. We did not need to take any action. The alert was displayed over all other windows and persisted until we closed it. When multiple threats were detected, only a single alert was shown.



Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, a TotalAV pop-up alert invited us to scan the device for threats; this included an option to disable such scan prompts in future. We declined to run a scan, and opened the drive in Windows File Explorer. TotalAV immediately showed a detection alert, and deleted the malware samples on the drive within a couple of seconds, making it impossible to copy any of them to the test PC (or run an execution check). We would describe this as exemplary behaviour for a security program.

When we scanned the USB drive via Windows Explorer's right-click menu, TotalAV showed us a list of the malicious files found. The default action for each detected file – which can be changed on an individual basis – was set to Quarantine. We simply had to click Quarantine All to deal with the detected threats. TotalAV then displayed the message Malware removed successfully. All the malware samples were deleted from the USB drive.

Scan options

You can run a *Smart Scan* from the button of the same name on the home page. The description states that this also checks for performance and privacy issues, and removes duplicate files. *Malware Scan* and *Quarantine* can be found by clicking *Malware Protection* (the shield icon in the top left-hand corner). For *Malware scan* there is a choice of *Quick Scan, System Scan,* and *Custom Scan*. You can also scan a local drive, folder or file using the right-click menu in Windows File Explorer. Although this feature supposedly also allows you to scan network shares, we found that doing so did not detect any malware.

In the program's settings, you can change a number of options, such as whether to scan removeable drives, type and time of scheduled scans, and action to be taken when malware is discovered. Exclusions can also be set here. We did not find any settings for potentially unwanted programs.

Quarantine

The quarantine function is opened by clicking *Malware Protection*, then *Quarantine*. For each item, the file name, threat name and date/time the threat was quarantined is displayed. You can easily select individual or multiple items, and delete or restore these.

Logs

There is no separate logs feature, though you can see the day and time threats were encountered in *Quarantine*.

Help

The help feature can be accessed by clicking the *?* symbol in the top right-hand corner of the program window. This opens the *Help Center* page of Total AV's website. There are tiles for different topics; by clicking on the *Technical Support* tile, you will see further tiles for different topics related to the antivirus program, namely *Setup*, *Configuration and Setting*, *Malware* and *Password Vault*. For each topic, there are simple explanations and instructions, generously illustrated with annotated screenshots and videos.

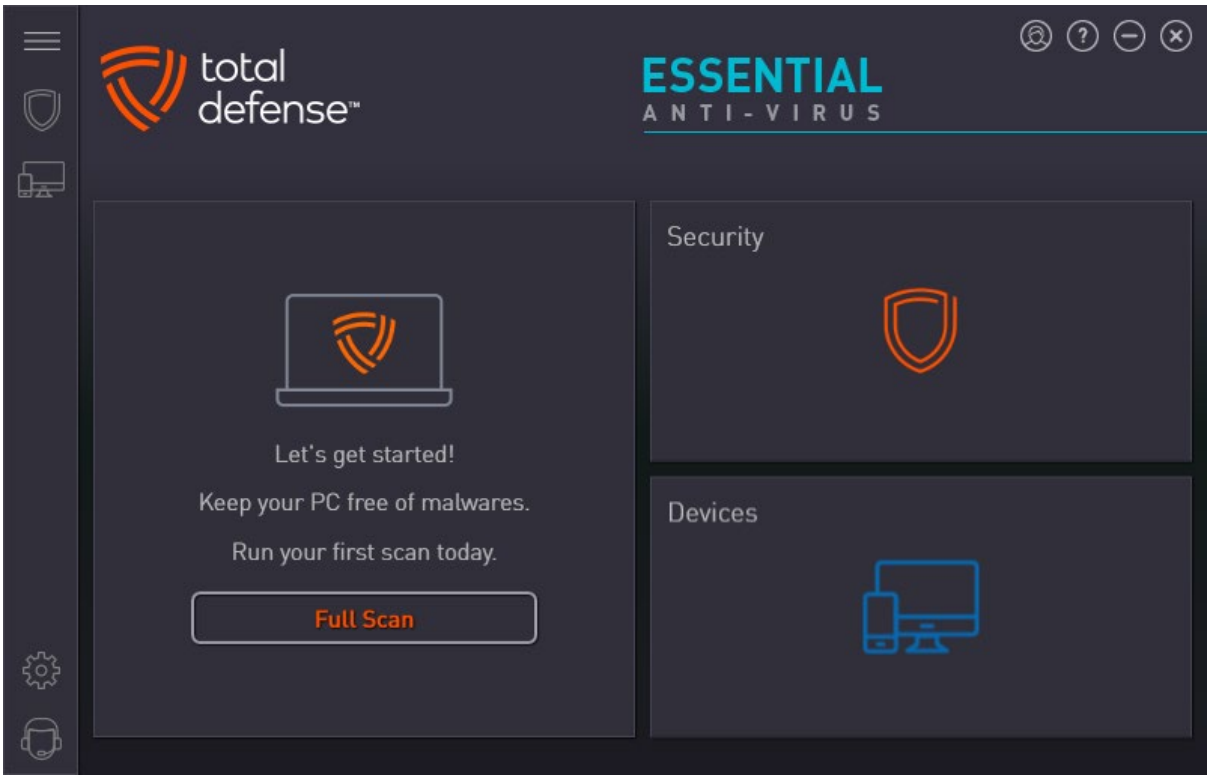
Access control

Standard Windows users cannot disable protection features, or uninstall the program. They can however change other settings.

Other points of interest

- TotalAV's online account lets you easily share your licences with family, friends or colleagues. On the *Share Licenses* page, you can send invitations by email. When the recipient installs the software, their device will show up on the *Dashboard* page of the console, and can be managed from there.
- We note that if you wish to cancel your TotalAV subscription, TotalAV advises you to contact their support service before uninstalling the product.

Total Defense Essential Anti-Virus



About the program

Total Defense Essential Anti-Virus is a paid-for security program, which offers malware and phishing protection features; the Privacy Protection feature monitors which apps use the camera/microphone. You can find out more about the product on the vendor's website: https://www.totaldefense.com/shop/anti-virus

Summary

Total Defense Essential Anti-Virus is easy to install, and presents a very simple program interface that makes important functions easy to find. In our functionality check, external USB drives were automatically scanned on connection. The help articles are clear and well-illustrated.

Setup

The installer allows you to change the language and set the installation folder und *Custom Install*. The installation is quick and requires no further intervention from the user. After the installation is finished, the program checks the product status, updates malware-signatures, and runs a performance optimization scan; this takes a few minutes.

System Tray icon

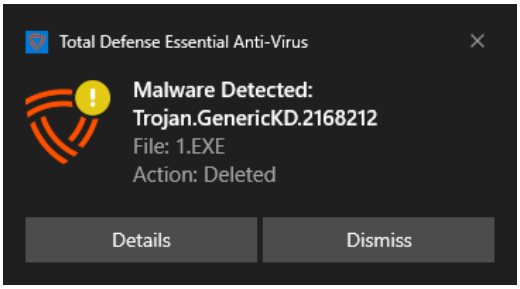
The System Tray icon menu lets you open the main program window, check for updates, run a quick scan, and pause real-time protection.

Security status alert

When we disabled real-time protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Fix all*.

Malware detection alert

When a malicious file was detected in our functionality check, Total Defense displayed the alert shown below. We did not need to take any action, and the alert closed after a few seconds. Clicking *Details* showed the applicable entry on the program's log page.



When multiple malicious files were detected at the same time, Total Defense displayed one alert for each of these.

Malware detection scenarios

We performed an Execution Check with Total Defense, which involved running our 5 malware samples from a USB flash drive connected to the test PC. All the malicious files were immediately detected and deleted, without any being able to start a process. When we attached a USB flash drive with some malware samples and clean files to our test PC, Total Defense automatically started a scan of the drive – an obviously safe option for non-expert users. In order to conduct our test as planned (i.e. copy file to the system), we cancelled this scan, and opened the drive in Windows Explorer. Total Defense did not take any action at this stage. However, when we tried to copy the drive's contents to the Windows Desktop, the security program prevented the malicious files from being copied. Total Defense displayed one alert for each of the malicious files, although these alerts did not start appearing until over a minute after the copy process had completed. We noted extremely high CPU usage during this time. When we scanned the USB drive via Windows Explorer's right-click menu, Total Defense displayed the notification *Scan Complete - Threats Detected and Resolved*. There was an option to view further details of the scan. We consider this to be a good solution, as no user decision was required. All the malware samples were deleted from the USB drive.

Scan options

You can run a full scan from the *Home* page of the program. Opening the *Security* tab allows you to run a quick, full, system or custom scan. The *Suspend Scans* button on the same page temporarily deactivates real-time protection for a specified number of minutes. You can scan a local drive, folder or file, or a network share, using Windows Explorer's right-click menu. In the *Security**Settings**Scanner* tab you can set the level of scanning protection by adjusting the *Scan* Options slider. Available options are *Low, Recommended* (default), *High* or *Custom*; Total Defense tell us that the default setting enables PUA detection. Selecting Custom lets you decide whether to scan network, archive, and hidden files, and whether suspicious files should be treated as infected.

Quarantine

This feature is found on the *Security* page, *Quarantine* tab (shield icon with a lock). It shows the date and time of detections along with the file name. Click on an item shows further details, such as threat name and type, along with the action taken. You can select individual quarantined files, or all together, and restore or delete them from here.

Logs

The *Reports* tab of the *Security* page displays a list of threats found, along with the detection date/time, and scan type that detected them. This can be displayed as a summary, showing how many of each threat type has been blocked.

Help

Clicking the question-mark icon in the top right-hand corner of the window opens the *About* page. Here you can click *Support Info* and then *Online Support*. This opens the support page of the vendor's website. If you click *Product Support*, a searchable FAQs page opens. Each article provides simple, step-by-step instructions for the task in question, generously illustrated with annotated screenshots.

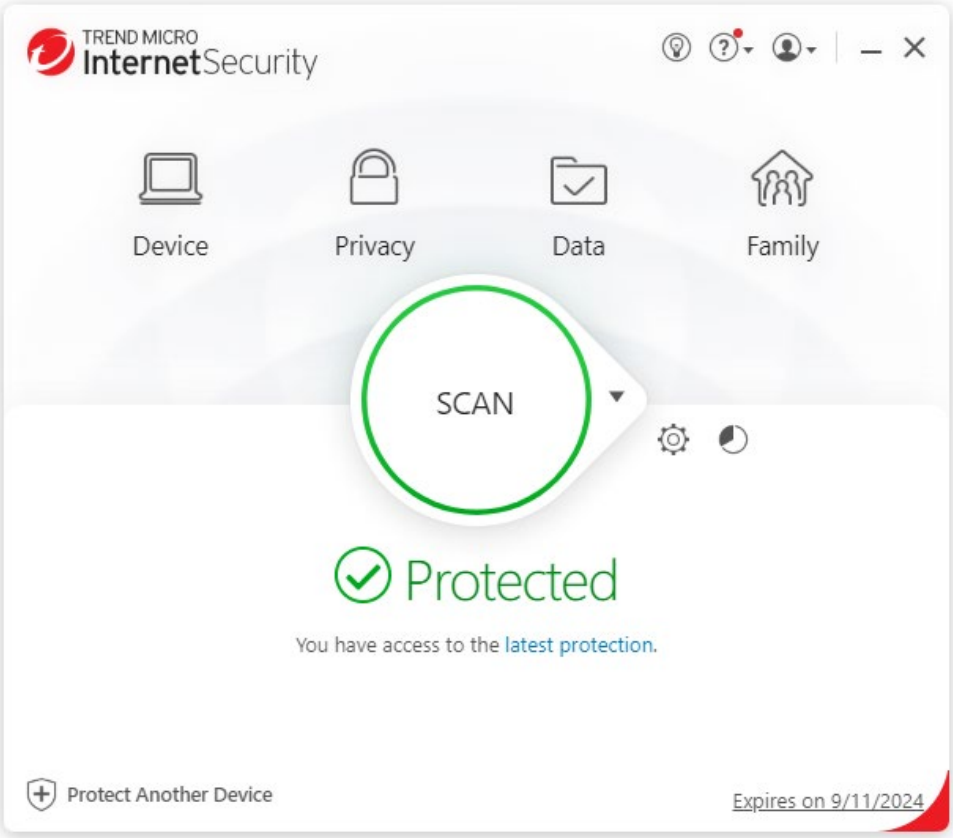
Access control

On the *Console* tab of the *Settings* page, you can prevent other users disabling protection or changing other security settings. If you enable the *Restrict access to antimalware configuration* option, all users will have to enter the password for the Total Defense account in order to change the AV settings. The same tab also allows you to control access to the *Devices* page, via the *Restrict access to devices configuration* option.

Other points of interest:

- You can also use the right-click menu to exclude a drive, folder or file from scans.
- The *Devices* page shows all the devices you have installed using the same account. For each device, you can see device type (e.g. PC); installed product (e.g. AntiVirus); security status; dates of last update and last scan; number of threats resolved. You can also change a device's name here, change the avatar representing its user, or delete the device to free up its licence.
- We observed long periods of extremely high CPU usage while conducting our malware detection checks with Total Defense. We suggest that this may explain the significant delay in displaying malware detection alerts in our USB Copy Check.

Trend Micro Internet Security



About the program

Trend Micro Internet Security is a paid-for security program. In addition to anti-malware features, it includes a ransomware shield, parental controls, secure erase feature, and a secure browser mode for financial transactions. You can find out more about the product on the vendor's website: https://www.trendmicro.com/en_us/forHome/products/internet-security.html

Summary

The program is very easy to install, and the simple user interface makes important features easy to find. Safe default settings are provided. In our functionality check, Trend Micro's highly sensitive on-access protection proactively deleted malware as soon as we opened it in Windows File Explorer. We liked the persistent malware and status alerts, and the online manual is simple and clear.

Setup

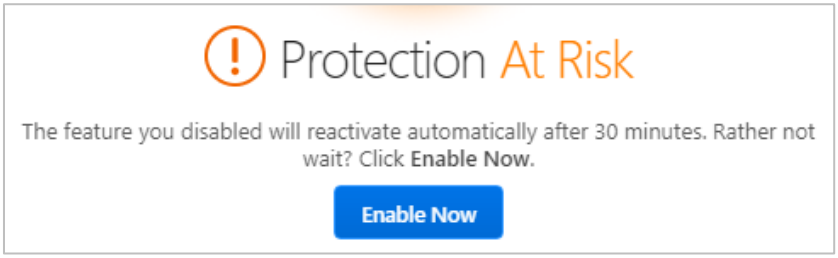
After launching the installer, you have to accept the license agreement, privacy and data collection notice. The setup wizard asks you to enter a licence key or opt for the free trial. Other than this, there are no decisions to make. At the end of the wizard, you are invited to set up the ransomware shield. By default, this covers Windows' Documents, OneDrive and Pictures folders, but you can add further folders if you want.

System Tray icon

The System Tray icon menu lets you open the main window, run a scan, check for updates, disable/enable protection, start mute silent mode, check your Trend Micro account and subscription, run a troubleshooting tool, and quit the program.

Security status alert

When we disabled protection in the program's settings, an alert was shown on the home page (screenshot below). We were able to reactivate the protection easily by clicking *Enable Now*.



An additional pop-up alert (screenshot below) was shown above the System Tray. This persisted until we closed it.

Malware detection alert

When a malicious file was detected in our functionality check, Trend Micro displayed the alert shown below. We did not need to take any action. The alert persisted until we closed it.

Clicking *More details* opened the program's scan log page, showing date and time of detection, file name and path, detection name and action taken, for each item. When multiple malicious files were detected at the same time, Trend Micro showed just one alert box.

Malware detection scenarios

When we attached a USB flash drive with some malware samples and clean files to our test PC, Trend Micro did not prompt us to scan the device. However, as soon as we opened the drive in Windows Explorer, the security program began deleting the malware samples, and displayed a single detection alert, which showed the (rapidly increasing) number of detections.

Trend Micro deleted the malware samples on the drive within about 10 seconds. Consequently, we did not have enough time to copy them to the test PC (or run an execution check). We would describe this as excellent behaviour for a security program. When we scanned the USB drive via Windows Explorer's right-click menu, Trend Micro displayed the notification *All Threats Resolved*, and showed the numbers of *Files scanned* and *Threats resolved*. There was an option to display further details. We consider this to be a good solution, as no user decision was required. All the malware samples were deleted from the USB drive. When we opened a writeable network share containing malware samples and clean files, Trend Micro displayed a detection alert and started gradually deleting the source malicious files from the shared folder, which is commendable. We were able to copy some of the malware samples to the Desktop of the test PC; Trend Micro deleted these about 30 seconds after the copy procedure had completed.

Scan options

The *Scan* button in the main program window runs a quick scan. Clicking the small down arrow to the right of this button gives you the choice of quick, full and custom. Scans can be scheduled from the program's settings dialog. By default, a smart schedule is used, which starts appropriate scans based on your computer usage. You can also scan a local drive, folder or file, or a network share, from Windows Explorer's right-click menu. The detection of PUA is enabled by default and can configured under *Settings\Scan Preferences*., you can configure detection of PUAs (enabled by default). The *Exception Lists* page of the settings lets you add scan exclusions.

Quarantine

The quarantine can be opened using the pie-chart symbol to the right of the *Settings* icon. The page shows a summary of threats found, grouped by type (such as *ransomware, web threats, computer threats)*. Clicking *See more details*, you can see a log of individual security-related events for each of these. Selecting *Viruses* from the drop-down menu, shows a list of malware detections, with the date and time of detection, file name and path, threat name, and action taken. Clicking on an entry in this list opens a panel with further information. If the malware concerned was quarantined (Trend Micro labels these files as removed), this details pane will show a *Restore* button. We suggest that this procedure is rather complicated, and could be made easier for non-expert users.

Logs

There is no separate logs feature, quarantine and logs are combined in the *Security Report* page.

Help

Clicking the *?* menu, *Product Support* opens the program's online manual. The first page has an overview of the program's main functions. Clicking the *?* in other program windows, opens the corresponding help page. There are simple explanations and instructions, some being well illustrated with screenshots.

Access control

Standard Windows users can disable protection features, but not uninstall the program. Under *Other Settings\Password*, you can password protect the program to prevent other users changing the settings. You also need to provide a password hint and an email address for resetting the password. Trend Micro Internet Security requires you to set up password protection before allowing you to disable protection via the System Tray icon menu, but not via the program's settings.

Featurelist Windows (as of December 2023)	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL
Product name	Avast Free Antivirus	AVG AntiVirus Free	Avira Prime	Bitdefender Internet Security	ESET Internet Security	F-Secure Internet Security	G Data Total Security	K7 Total Security	Kaspersky Standard	McAfee Total Protection	Microsoft Defender	Norton Antivirus Plus	Panda Free Antivirus	TotalAV Antivirus Pro	Total Defense Essential Anti-Virus	Trend Micro Internet Security
Supported Program languages	All	English, Czech, Danish, German, Spanish, French, Hungarian, Indonesian, Italian, Japanese, Korean, Malaysian, Dutch, Norwegian, Polish, Portuguese, Russian, Slovak, Serbian, Turkish, Chinese	English, German, Italian, French, Spanish, Portugese, Russian, Dutch, Turkish, Japanese, Chinese, Indonesian	English, French, German, Dutch, Spanish, Italian, Romanian, Portuguese, Polish, Greek, Vietnamese, Turkish, Korean , Czech, Japanese, Hungarian, Thai	English, Arabic, Bulgarian, Czech, Danish, German, Greek, Spanish, Estonian, Finnish, French, Hebrew, Croatian, Hungarian, Chinese, Italian, Japanese, Kazakh, Korean, Lithuanian, Dutch, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Serbian, Swedish, Thai, Turkish, Ukrainian, Vietnamese, Latvian, Indonesian	English, Bulgarian, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English	English, Arabic, French, Bulgarian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lituanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Chinese, Spanish, Swedish, Thai, Turkish, Ukrainian, Vietnamese	English, Chinese, Danish, Dutch, Finnish, French, German, Greek, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, Dutch, Portuguese, Czech, Danish, German, Spanish, Italian, Norwegian, Polish, Russian, Finnish, Swedish, Turkish, Chinese, Japanese, Korean, Arabic, Hebrew	English, French, German, Japanese, Spanish, Italian, Dutch, Swedish, Finnish, Norwegian, Danish, Portuguese, Czech, Polish, Hungarian, Romanian, Slovak, Russian, Greek, Turkish, Chinese, Korean, Arabic, Hebrew	English, Bulgarian, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Russian, Chinese, Slovak, Slovenian, Spanish, Swedish, Turkish	English, Danish, Dutch, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish, Turkish	English, Spanish	English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Dutch, Danish, Norwegian, Swedish, Indonesian, Korean, Thai, Turkish, Vietnamese
Third-party scan engine included	proprietary	Avast	proprietary	proprietary	proprietary	Avira	Bitdefender	proprietary	proprietary	proprietary	proprietary	proprietary	proprietary	Avira	Bitdefender	proprietary
Protection																
Scans file on execution	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Scans files on demand	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-access file scan after Internet download (by DEFAULT)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-access file scan while copying/moving files (by DEFAULT)	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Prevents access to phishing and other malicious websites	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●
Detects also threats for e.g. Android, Mac, Linux	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●
Detection of potentially unwanted applications (PUA) turned ON by DEFAULT	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Is the online malware detection the same as offline				●	●		●	●							●	
Additional features (selection chosen by AV-Comparatives)																
Multi-device protection / Multi-platform licensing	●	●	●	●	●	●	●		●	●	●			●	●	●
Firewall	●	●	●	●	●		●	●	●	●	●	●				
WiFi protection / Home Network Protection	●	●	●	●	●			●		●				●		●
Browser cleanup / Privacy cleaner / File Eraser	●	●	●	●	●		●	●	●	●	●			●		●
Rescue disk	●	●	●	●	●		●		●		●	●	●			●
Scans HTTPS traffic	●	●	●	●	●	●	●	●	●			●			●	●
Secure Browser / banking protection / Private Browsing	●	●	●	●		●	●		●		●	●				●
Device Access Control / USB Protection	●	●	●	●			●	●	●		●		●		●	
Software Updater / Vulnerable-Software Reporter	●	●	●	●				●	●	●	●				●	
Parental Control				●	●	●	●	●		●	●					●
Webcam / Audio Protection	●	●		●				●	●			●			●	
Anti-Spam				●	●		●	●			●					●
Password Manager			●	●			●			●		●				
Data-Breach checker	●	●	●							●				●		
VPN (unlimited)			●							●						
Ad-Blocker / Anti-Tracker			●	●				●	●							
Secure Keyboard / Virtual Keyboard				●				●	●		●					
Application Manager								●	●		●			●		
Malware Removal support guarantee (money-back)										●		●			●	
Backup							●			●		●				
Folder Shield / Data Locker	●	●					●	●			●					●
Support options (may vary depending on location and language)																
Online Help	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Support Forum	●	●	●	●	●	●		●	●	●	●	●	●			●
Phone Support			●	●	●	●	●	●	●	●		●		●	●	●
Email Support			●	●	●		●	●	●					●	●	●
Downloadable User Manual (PDF)				●		●					●	●				●
Supported languages (of support)	English, French, Czech, German, Italian, Spanish, Russian, Dutch, Japanese, Portuguese, Polish	English, German, Czech, French, Italian, Spanish, Portuguese, Dutch, Japanese, Polish	English,German, French, Italian, Portuguese, Spanish	English, French, German, Romanian, Portuguese, Italian, Spanish	All	English, Bulgarian, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, German, French, Italian, Spanish, Portuguese, Dutch, Polish	English, Hindi, and Indian regional languages	English, Cantonese, Chinese, French, German, Greek, Hindi, Italian, Japanese, Polish, Portuguese, Romanian, Russian, Spanish, Turkish.	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian	English, Chinese, German, French, Portuguese, Spanish, Turkish, Polish, Danish, Dutch, Finnish, Greek, Italian, Norwegian, Romanian, Russian, Swedish, Slovenian, Hungarian	English, Spanish	English, Dutch, Danish, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish, Turkish	English	English, Japanese, Chinese

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(January 2024)